South Carolina Law Review

Volume 49
Issue 4 *SYMPOSIUM: CONDUCTING BUSINESS OVER THE INTERNET*

Article 6

Summer 1998

Electronic Commerce on the Internet and the Statute of Frauds

R. J. Robertson Jr.
Southern Illinois University School of Law

ELECTRONIC COMMERCE ON THE INTERNET AND THE STATUTE OF FRAUDS

R. J. ROBERTSON, JR.*

I. INTRODUCTION 789
II. TERMINOLOGY 790
III. THE BENEFITS AND PITFALLS OF ELECTRONIC COMMERCE 793
A. *The Benefits of Electronic Commerce* 793
B. *The Pitfalls of Electronic Commerce* 794
C. *Electronic Commerce and Legal Rules Premised on Paper-Based Commerce* 796
IV. ALTERNATIVE METHODS OF ACCOMMODATING THE STATUTE OF FRAUDS AND ELECTRONIC COMMERCE 797
A. *Allow the Courts to Determine Whether Electronic Commerce Agreements Satisfy the Statute of Frauds* 797
1. *The Telegraph* 798
2. *The Telex or Telecopier* 800
3. *The Telefacsimile (Fax) Machine* 801
4. *Tape Recordings* 803
5. *Computer Records and Other Writing Issues* 804
6. *Lessons from Cases Involving Earlier Technologies* 807
B. *Repeal the Statute of Frauds* 809
1. *The Functions of Form and the Requirement of a Signed Writing* 810
2. *The Dysfunction of Form and the Requirement of a Signed Writing* 812
3. *Electronic Commerce and the Functions and Dysfunctions of Form* 812
a. *The Functions of Formal Requirements in Electronic Commerce* 813
b. *The Dysfunctions of Form in Electronic Commerce* 814
C. *Amend the Statute of Frauds to Validate Electronic Commerce* ... 815
1. *Legislative Efforts to Equate Electronic Records*

---

* Associate Professor of Law, Southern Illinois University School of Law. A.B. 1973, J.D., *cum laude*, 1976, University of Missouri-Columbia. The author thanks Rob Evola, Allen Devary and Patrick Pericak for their helpful research assistance. The author is a member of Illinois Attorney General Jim Ryan's Commission on Electronic Commerce and Crime which has recently drafted the Illinois Electronic Commerce Security Act. Although the author has greatly benefited from the discussions among members of the Commission, the opinions expressed herein are the author's alone and do not necessarily reflect the opinions of the Commission, Attorney General Ryan, or other members of the Commission.

with Signed Writings 816
a. The Uniform Commercial Code 816
b. The Uniform Electronic Transactions Act 818
c. State Law Developments 819
(1) The Utah Model: Validating Only Electronic Messages with Digital Signatures 819
(2) The Georgia Model: A Narrow Validation of Records with "Electronic Signatures" 822
(3) The Florida and Illinois Model: Open-Ended Validation Records with Electronic Signatures 822
d. Analysis of the Various Models of Equating Electronic Records with Signed Writings 824
2. Legislative Efforts Regarding Security Procedures Used to Verify the Source and Content of an Electronic Message 827
a. The Uniform Commercial Code 828
b. The Uniform Electronic Transactions Act 830
c. State Law Developments 832
(1) The Utah Approach: Evidentiary Presumptions Based on Digital Signatures 832
(2) The Florida and Georgia Approach: No Provision for Evidentiary Issues 832
(3) The Illinois Approach: An Intermediate Position ... 833
d. Analysis of the Various Approaches to Verifying the Source and Content of an Electronic Message 835
(1) Is it Appropriate to Treat Electronic Signatures and Records Verified by Security Procedures Differently from Others? 835
(2) What Security Procedures Are Sufficiently Reliable to Merit Special Treatment? 837
(a) Digital Signatures Alone 837
(b) Security Procedure Agreed to by the Parties 839
(c) Security Procedures Previously Agreed to by the Parties and Other Reliable Security Procedures 841
(3) Is an Evidentiary Presumption a Proper Way to Encourage the Use of Security Procedures? 844
VI. CONCLUSION 846

I. INTRODUCTION

In recent years, technological developments have brought about a revolution in communication and business practices, centering on the use of personal computers connected through a web of networks commonly known as the "Internet." This revolution has led to increased efficiency for businesses and consumers seeking to purchase or sell goods, services, or intangibles. However, the increased use of personal computers in commerce faces barriers based on legal concepts that were developed at a time when the technology could not even have been imagined.

The principal perceived legal barrier to the development of electronic commerce on the Internet is the Statute of Frauds.[1] First enacted in England more than three hundred years ago, this much-maligned,[2] yet durable, statute was subsequently enacted, in substantially unchanged form, in every state. The Statute of Frauds conditions the enforceability of certain types of promises on the formal requirements of a "writing" that is "signed" by the person against whom the promise is sought to be enforced. Because much electronic commerce is predicated on the exchange of electronic messages, without the production of a paper record of the messages, a requirement of a "signed writing" evidencing the transaction is widely believed to discourage the use of these efficient technologies. Accordingly, many commentators have called for the repeal or substantial abolition of the Statute of Frauds as it relates to electronic commerce transactions[3] or for amendment of the Statute of Frauds to validate these transactions.[4] Indeed, forty-three states have either enacted or are considering legislation affecting the Statute of Frauds as it relates to electronic commercial transactions.[5]

---

1. Practical impediments exist as well, including the attitudinal reluctance to use computers in commercial transactions. This attitude results, in part, from highly publicized incursions of computer networks for fraudulent or malicious reasons. Some notable examples are listed in WARWICK FORD & MICHAEL S. BAUM, SECURE ELECTRONIC COMMERCE § 1.1, at 3-5 (1997). Another impediment is the absence of a secure method of payment for items purchased on the Internet. However, recent developments indicate that this latter barrier may soon disappear. VISA and MasterCard are jointly experimenting with a venture known as the Secure Electronic Transaction (SET) protocol which involves the encrypted transmission and confirmation of credit card numbers in such a way that the merchant can verify the validity of the credit card without knowing the credit card number. For a brief description of the SET protocol, see *id.* § 7.8, at 303-06.

2. *See, e.g.*, Francis M. Burdick, *A Statute for Promoting Fraud*, 16 COLUM. L. REV. 273, 273-74 (1916); E. Rabel, *The Statute of Frauds and Comparative Legal History*, 63 L.Q. REV. 174, 186-87 (1947); James Fitzjames Stephen & Frederick Pollock, *Section Seventeen of the Statute of Frauds*, 1 L.Q. REV. 1, 5-8 (1885); Hugh Evander Willis, *The Statute of Frauds—A Legal Anachronism* (pts. 1 & 2), 3 IND. L.J. 427, 528 (1928).

3. *E.g.*, Marc E. Szafran, Note, *A Neo-Institutional Paradigm for Contracts Formed in Cyberspace: Judgment Day for the Statute of Frauds*, 14 CARDOZO ARTS & ENT. L.J. 491, 508 n.73 (1996).

4. *E.g.*, Deborah L. Wilkerson, Comment, *Electronic Commerce Under the U.C.C. Section 2-201 Statute of Frauds: Are Electronic Messages Enforceable?*, 41 U. KAN. L. REV. 403, 426-27 (1992).

5. A current list of state statutes, both enacted and proposed, can be found at the web site of the Chicago law firm of McBride, Baker & Coles. *Summary of Electronic Commerce and Digital*

In discussing the issues raised by electronic commerce on the Internet and the Statute of Frauds, this Article first defines some key terms that will be used in this Article and then discusses the benefits and hazards of various forms of electronic commerce. Next, this Article examines three legislative alternatives to accommodate the needs of electronic commerce and the Statute of Frauds: (1) do nothing and allow the judiciary to determine whether electronic commerce transactions satisfy the existing requirements of the Statute of Frauds; (2) repeal the Statute of Frauds, either altogether or as to electronic commerce transactions; or (3) amend the Statute of Frauds to validate all, or some, forms of electronic commerce transactions. This Article concludes that only the third of these alternatives is practicable and then reviews and evaluates a number of legislative initiatives amending the Statute of Frauds to accommodate electronic commerce.

II. TERMINOLOGY

This Article employs a number of terms to describe various forms of electronic transactions. For purposes of this Article, an "electronic commerce" transaction is one that is consummated by two or more persons (or by two or more computers programmed by persons) who exchange messages regarding an agreement through an electronic messaging system, and who have no expectation that a paper record of the transaction will be generated or retained by either party. Hence, the term "electronic commerce" does not include messaging systems like telegraph, telex, or facsimile machines, all of which also involve electronic transmission of messages, because these technologies ordinarily produce a message on paper.[6] Likewise, it does not include documents created by one person, such as wills or trusts, even though such documents may have legal consequences. Finally, it does not cover the electronic filing of information with a government entity as required or allowed by law.

As defined, electronic commerce has two distinct subsets. The first is Electronic Data Interchange (EDI). "EDI is the movement of electronic business messages, such as purchase orders, from computer to computer."[7] EDI is distinguished from other forms of electronic messaging because its messages are structured and coded in accordance with a standard previously agreed upon by sender and recipient.[8] The

---

Signature Legislation (last modified Mar. 10, 1998) <http://www.mbc.com/ds_sum.html>.

6. The foregoing is not entirely accurate, given the recent development of fax modems that transmit data which emulate a fax but store such data on a computer disk, and the increasing use of computers as telex terminals. BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE §§ 1.1.1, 1.1.3 (2d ed. 1996). However, because the majority of fax and telex transmissions produce a paper record, they do not pose the problems presented by pure, paper-free "electronic commerce" and will not be included in that term.

7. *Id.* § 1.1.4, at 1:8; *see also* FORD & BAUM, *supra* note 1, § 2.4, at 27 (defining EDI as "the computer-to-computer exchange of business transactions, such as purchase orders, invoices, and payment advices within large industrial communities or government.").

8. WRIGHT, *supra* note 6, § 1.1.4, at 1:8.

standard is a language that adheres to a prescribed syntax so that each item of data is transmitted in a prescribed order and is surrounded by a computer-generated code that operates to delineate the different items of data.[9] EDI transactions are designed to allow a receiving computer to automatically transfer the data into other application programs, making it unnecessary for a human to receive the message and then manually key the data into another application program.[10] EDI transactions are limited to transactions between businesses and require some prior agreement between the parties in order to establish which of the available standards the EDI "trading partners" will use.[11] EDI transactions generally are conducted over value-added networks[12] and historically have not used Internet protocols.[13] Although EDI transactions will be briefly discussed in this article, they do not pose many of the problems posed by less structured electronic commerce transactions conducted over the Internet.

Electronic commerce not involving EDI can be called "open electronic commerce," which is "characterized by Internet-based, ubiquitous commerce without pre-negotiated, customized, bilateral agreements" between participants.[14] Open electronic commerce transactions take one of two forms: The first is electronic mail (e-mail), the transfer of messages from one computer to another, usually in alphanumeric character messages intended for human reading;[15] the second is many-to-many communication, which "makes a mass of information available to remote computer users in a real-time, interactive mode."[16] The primary example of many-to-many communication is the World Wide Web, a network of interconnected computers on the Internet.[17] Electronic commerce on the World Wide Web is a relatively recent development. Unlike EDI, which is used exclusively by businesses, open electronic commerce, either by e-mail or on the World Wide Web, is capable of being used by both business persons and consumers who desire to sell and buy items.

Open electronic commerce transactions on the World Wide Web may, in turn,

---

9. *Id.*; *see also* Douglas Robert Morrisson, Comment, *The Statute of Frauds Online: Can a Computer Sign a Contract for the Sale of Goods?*, 14 GEO. MASON L. REV. 637, 641 (1992) (stating that "EDI tightly controls the sequence in which the data appear" to preserve the integrity of the data).

10. WRIGHT, *supra* note 6, § 1.1.4, at 1:8.

11. *See* FORD & BAUM, *supra* note 1, § 2.4, at 29.

12. These networks generally provide "data communications services and, in addition, assist their clients in such areas as software configuration, security, auditing, transaction tracing, and recovery of lost data," FORD & BAUM, *supra* note 1, § 2.4, at 27.

13. *Id.*

14. *Id.* at 29. Of course, it is possible for two entities to agree to conduct business with each other over the Internet in a non-EDI format. *See infra* text accompanying note 19.

15. WRIGHT, *supra* note 6, § 1.1.2, at 1:6.

16. *Id.* § 1.1.6, at 1:10.

17. *Id.* "The *Internet* is an international network of computers and computer networks connected to each other through routers using the TCP/IP protocols and sharing a common name and address space." HENRY H. PERRITT, JR., LAW AND THE INFORMATION SUPERHIGHWAY § 1.2, at 5 (1996).

take different forms.[18] One form would be repeated transactions between one seller and one buyer. For example, a buyer and seller might agree to conduct future transactions with each other over the Internet in a non-EDI format. In these circumstances, the parties would likely enter into an agreement similar to that used by EDI trading partners and will likely provide for the use of security procedures that will allow them to identify each other's messages in a reliable way.

A closely related form would be repeated transactions between one seller and a number of buyers. For example, a mail-order catalog business might operate a web site that could be used by its customers to purchase items. In such a case, the seller and each of its buyers would likely agree that the buyer would use some form of security procedure (such as a PIN number) in order to identify the buyer to the seller's computer when placing an order.[19]

Finally, there is at least the prospect of what can be called stranger-to-stranger transactions on the Internet. In these instances, typically neither the buyer nor the seller will have had prior dealings with each other and, in many cases, the only dealing they ever will have is the sale of a single item in an isolated transaction. This situation poses the greatest risk of fraud and misunderstanding.

The term "Statute of Frauds" is misleading because it suggests that there is a single statute defining all the promises that must be evidenced by a signed writing in order to be enforceable; in fact, every state has numerous statutes requiring various types of agreements to take such form. The traditional Statute of Frauds is modeled after the English statute of 1677 and ordinarily requires a memorandum signed by the party against whom an action is brought to enforce specified categories of promises.[20] However, the most commercially significant writing requirement for contracts is section 2-201 of the Uniform Commercial Code (U.C.C.). This provision requires some "writing"[21] "signed"[22] by the person against whom enforcement is sought in order for a contract for the sale of goods at a price of $500 or more to be enforceable.[23] Furthermore, in virtually all states there are different statutes that require other types of promises to be in some written or signed

---

18. For a description of various forms of open electronic commerce, and a helpful taxonomy of possible authentication procedures that would be used in these forms, see Jane Kaufman Winn, *Open Systems, Free Markets and Regulation of Internet Commerce*, 72 TUL. L. REV. (forthcoming 1998). This article is available online at <http://www.smu.edu/~jwinn/esig.htm>.

19. Professor Winn describes a system involving both of these forms of open electronic commerce as a "closed-bilateral" one. *Id.*

20. A typical Statute of Frauds in the United States includes contracts for the sale of an interest in real property; contracts that cannot be performed within one year of the date of their making; contracts whereby one person agrees to answer for the debts of another; and other miscellaneous promises such as marriage promises and brokerage agreements. *See, e.g.*, CAL. CIV. CODE § 1624 (West Supp. 1998); 740 ILL. COMP. STAT. 80/1 (West 1993 & Supp. 1997).

21. "'[W]riting' includes printing, typewriting or any other intentional reduction to tangible form." U.C.C. § 1-201(46) (1995).

22. "'Signed' includes any symbol executed or adopted by a party with present intention to authenticate a writing." U.C.C. § 1-201(39) (1995).

23. U.C.C. § 2-201(1) (1995).

form to be enforceable.[24]

Although there are substantial differences between the various forms of these statutes and their requirements, for purposes of this article, the term Statute of Frauds refers, collectively, to all state statutes requiring some writing or note or memorandum that is signed by or bears the signature of some person as a requirement for the enforceability of a promise or set of promises.[25] To avoid redundancy, this article will use the words "writing" and "signed" to encompass all similarly-phrased requirements.

III. THE BENEFITS AND PITFALLS OF ELECTRONIC COMMERCE

A. The Benefits of Electronic Commerce

EDI and open electronic commerce transactions produce similar benefits for both suppliers and purchasers of items sold in electronic commerce transactions. Both forms of communication cut costs by eliminating inefficient paper shuffling and storage.[26] Both allow commercial entities to react more swiftly to changing conditions by altering pricing to reflect supply and demand in real-time.[27] Both allow essentially instantaneous responses to needs of the other party.

However, EDI, as the more structured and older technology, has some benefits not yet translatable into open electronic commerce transactions. For example, EDI utilizes a prescribed syntax based on public EDI standards. Accordingly, the receiving computer can automatically transfer the structured and coded data "into diverse application programs such as inventory management software."[28] This reduces the possibility of data-entry errors by a human recipient and expedites the process of fulfilling orders, shipping products, and accounting.[29] Likewise, EDI cuts costs by eliminating "redundant keying of information into computers."[30] It also

---

24. For example, the Illinois General Assembly has enacted statutes requiring the following types of contracts, *inter alia*, to be evidenced by some writing: contracts with a credit services organization, 815 ILL. COMP. STAT. ANN. 605/7 (West 1993); contracts for dance studio services, 815 ILL. COMP. STAT. ANN. 610/4 (West 1993); contracts for the payment of royalties from music, 815 ILL. COMP. STAT. ANN. 637/15 (West Supp. 1997); and contracts for physical fitness services, 815 ILL. COMP. STAT. ANN. 645/4 (West 1993).

25. Outside the U.C.C., the terms "memorandum" or "note" are frequently used instead of writing and the term "subscribed" is occasionally used instead of signed. Ordinarily, none of these terms are defined in the Statute of Frauds itself and must be interpreted by courts as individual disputes arise. Although some courts have found significant differences between a requirement that the contract be either in writing or evidenced by a note or memorandum, they are unimportant for purposes of this article. *See generally* 4 SAMUEL WILLISTON & WALTER H. E. JAEGER, A TREATISE ON THE LAW OF CONTRACTS § 567A, at 12-13 (3d ed. 1961).

26. WRIGHT, *supra* note 6, § 2.4, at 2:7.

27. *Id.*

28. *Id.* § 1.1.4, at 1:8.

29. *Id.*

30. *Id.* § 2.4, at 2:7.

helps businesses cut lead times and reduce inventories.[31] As a result, orders are more frequent, smaller in quantity, and less valuable, reducing the incentive to dispute a particular transaction.[32] "Because the standards cover a relatively inflexible set of transaction sets, EDI communications are much less likely to be ambiguous than free text transmissions" used in open electronic commerce transactions[33] which substantially reduces the likelihood of misunderstanding between EDI trading partners.

On the other hand, open electronic commerce has a number of advantages not present in EDI. EDI transactions are conducted between trading partners who have a history of prior transactions. Furthermore, the structure of EDI standards is such that it cannot be used as a form of advertising to reach new customers. However, the openness and lack of structure on the Internet, particularly the World Wide Web, allow interested buyers to surf the Web looking for sellers of an item, and sellers can advertise their products and services for sale to these potential buyers.[34] After finding a suitable product, the buyer can place an order, make payment and shipping arrangements, and receive some confirmation of the order, all without speaking to another human being or producing any paper record of the transaction. This openness allows sellers to create, and buyers to access, a market that is literally world-wide.

B. The Pitfalls of Electronic Commerce

EDI transactions have very few pitfalls. There is, of course, the possibility of data-entry errors or programming glitches at the sending computer, but these are no different than the chances of error in paper-based transactions.[35] The structure and codes that permeate EDI transactions, as well as the fact that these transactions are often conducted over secure networks, reduce the likelihood of malicious third-party intervention. EDI safeguards are very sophisticated, but for purposes of this article, need not be detailed.[36]

In order to understand some of the problems posed by open electronic commerce transactions other than e-mail, it is necessary to understand that these

---

31. *Id.* "EDI is the lifeblood of the just-in-time campaign in manufacturing and the 'Quick Response' techniques in retailing." *Id.*

32. WRIGHT, *supra* note 6, § 2.4, at 2:7.

33. YOCHAI BENKLER, RULES OF THE ROAD FOR THE INFORMATION SUPERHIGHWAY: ELECTRONIC COMMUNICATIONS AND THE LAW § 1.2[3], at 13 (1996).

34. FORD & BAUM, *supra* note 1, § 2.2, at 21.

35. A number of cases have reached different results concerning the legal effect of offers sent by telegram where the telegraph company enters a price or amount different from that directed by the offeror. *Compare* Ayer v. Western Union Tel. Co., 10 A. 495, 497 (Me. 1887) (offer valid), *with* Western Union Tel. Co. v. Cowin & Co., 20 F.2d 103, 104 (8th Cir. 1927) (offer invalid).

36. For excellent summaries of the reliability of EDI-transmitted data, see FORD & BAUM, *supra* note 1, § 5.6, at 172-73 (discussing internal EDI security mechanisms); WRIGHT, *supra* note 6, § 5.3, at 5:4-5:5 (discussing methods to ensure reliable EDI transmission).

transactions involve the transmission of information in digital form, rather than alphanumeric text files. Such information is represented in a binary series of zeroes and ones and may include items other than language, such as music and color.[37] "The most common manner in which binary files are transferred is called File Transfer Protocol" (FTP), which "allows the user to send complex files, as well as to retrieve data from sources, both public and private, that are not or cannot be presented in free text."[38]

"Digital representation strips information down to very simple building blocks—binary electric impulses" representing zeroes and ones.[39] This digital representation is mutable and can be manifested in different ways.[40] For example, digital representation of words can take the form of either text or speech.[41] As one writer has observed, "[t]he essence of a text can no longer be its unique combination of information and fixed form, for the knowledge that it conveys is mutable—to speech, sound or visual imagery."[42]

Because digital representation of information is so basic, human beings do not have immediate access to information stored and represented digitally.[43] We must use a mediating device, such as a computer screen, a video projection, an audio speaker, or a printed page.[44] In this sense, the information actually viewed or heard is never really original, because it is a representation of information stored in machine-readable form. On the other hand, the representation is an original in that every copy is an original and no original is not a copy.[45]

The other determining characteristic of digital information is its malleability. Because digital information comes in simple, building-block form,[46] users can receive the information and interact with it. Users "can transform its representation, they can add and subtract, cut and paste, copy and multiply, becoming producers as well as consumers of the message."[47] Unlike tangible items, such as paper, it is impossible to tell a copy of digital information from the original, and it is functionally impossible to tell that a digital message has been tampered with by someone other than the original sender.[48]

In addition to the inherent problems of storing and transmitting information in digital form, open electronic commerce transactions (including e-mail) lack the structure and coding associated with EDI transactions and are thus more likely to

37. BENKLER, *supra* note 33, § 1.2[2], at 11.
38. *Id.*
39. *Id.* § 2.1[1][a], at 23.
40. *Id.*
41. *Id.*
42. *Id.*
43. BENKLER, *supra* note 33, § 2.1[1], at 24.
44. *Id.*
45. *Id.*
46. *Id.* § 2.1[1][b], at 25.
47. *Id.*
48. *Id.* § 2.3[1], at 31-32.

give rise to ambiguity and misunderstanding. These transactions are conducted over open, insecure networks and it is impracticable to attempt to limit access to these networks. Because messages on the Internet are not sent over a single pathway, but are transmitted over a series of thousands of networks, a message must, necessarily, move from packet-switching node to node[49] on the Internet before reaching its final destination. The result is that any person with access to any intermediate node, can intercept, read, or alter an electronic message in a way that is undetectable by the recipient.[50]

Likewise, a person who receives an electronic message over the Internet will have great difficulty in reliably identifying the source of the message. "[I]t is relatively easy to 'spoof' a network into sending a communication with a 'return address' of someone other than the actual sender."[51] This possibility is complicated because open electronic commerce "contemplates one-time exchanges between parties who may have never dealt with each other before"[52] and have no meaningful way of establishing one's *bona fides* without an investigation that would be more expensive to undertake than the value of the transaction at issue. Finally, a computerized record of an open electronic commerce transaction can be easily and undetectably altered once it is stored in the recipient's computer.[53]

C. *Electronic Commerce and Legal Rules Premised on Paper-Based Commerce*

For all the foregoing reasons, the transmission of information over open networks and the storage of information in digital form is inherently less secure than transmitting and storing information on paper. Signed paper documents have a number of inherent security attributes, such as the semipermanence of ink embedded in paper, unique attributes of some printing processes, watermarks, the distinctiveness of individual signatures, and the limited ability to erase, interlineate or otherwise modify words on paper.[54] For years individuals and businesses have relied on these inherent security attributes to make a signed paper document a reliable basis for conducting business.

Although open electronic commerce transactions pose security risks to the participants not present in transactions utilizing signed paper documents, the advantages of open electronic commerce greatly outweigh those risks. However, the

---

49. Information on the Internet is transmitted in a string of data bits, known as a "packet." These packets are transferred according to layers of protocols that operate independently of each other. For an explanation of these different layers of protocols, see FORD & BAUM, *supra* note 1, § 2.1, at 15-17.

50. GARRY S. HOWARD, INTRODUCTION TO INTERNET SECURITY 207 (1995); Lorijean G. Oei, *The Legal Role of Information Security, in* ONLINE LAW: THE SPA'S LEGAL GUIDE TO DOING BUSINESS ON THE INTERNET 27, 32-33 (Thomas J. Smedinghoff ed., 1996).

51. Oei, *supra* note 50, at 32; *see also* HOWARD, *supra* note 50, at 207.

52. Oei, *supra* note 50, at 33.

53. *Id.*

54. FORD & BAUM, *supra* note 1, § 1.2, at 6.

Statute of Frauds presents a fundamental legal barrier to the expansion of electronic commerce. Notwithstanding the undoubted advantages of doing business electronically, even if the security risks can be minimized, many business persons remain unwilling to conduct business electronically so long as there is substantial doubt concerning the legal validity of agreements entered into electronically.[55] Hence, some accommodation between electronic commerce and the Statute of Frauds must be reached.

IV. ALTERNATIVE METHODS OF ACCOMMODATING THE STATUTE OF FRAUDS AND ELECTRONIC COMMERCE

State legislatures have three possible courses of action with respect to the Statute of Frauds and electronic commerce transactions: (1) do nothing, and allow the courts to determine, on a case-by-case basis, whether electronic commerce agreements satisfy the requirements of the Statute of Frauds; (2) repeal the Statute of Frauds, either altogether or with respect to electronic commerce transactions; or (3) amend the Statute of Frauds to validate all, or some, forms of electronic commerce transactions.

A. Allow the Courts to Determine Whether Electronic Commerce Agreements Satisfy the Statute of Frauds

Although computers are revolutionizing communications and commerce, it must be remembered that this is not the first revolution in communication since the advent of the Statute of Frauds. Over the years, courts have had to apply the provisions of the Statute of Frauds to a number of technological innovations that at the time must have seemed just as revolutionary as computers seem today. For more than 150 years, courts have interpreted the Statute of Frauds in a way that accommodated these innovations without legislative amendment. A legislature, therefore, could rationally decide that the courts alone are perfectly competent to determine the relationship between the Statute of Frauds and electronic commerce.

It should be remembered that, other than the U.C.C., the Statute of Frauds does not define what is meant by a "writing" or a "signing."[56] Hence, courts have frequently had occasion to interpret these terms in many earlier cases. Reviewing how courts have interpreted the Statute's requirements of a signed writing with respect to past innovations may assist in predicting how courts will interpret the Statute of Frauds with respect to electronic commerce.

---

55. *E.g.*, Geanne Rosenberg, *Legal Uncertainty Clouds Status of Contracts on Internet*, N.Y. TIMES, July 7, 1997, at D3.

56. 4 WILLISTON, *supra* note 25, § 567, at 5.

1. The Telegraph

In 1844, Samuel F. B. Morse sent the telegraphic message "What hath God wrought,"[57] thereby inaugurating a revolution in communications. It did not take long for the question of the legal effect of telegraphic messages to find its way into American courts. In *Durkee v. Vermont Central Railroad Co.*[58] an agent brought an action to recover a commission for his services pursuant to authorization sent by telegraph. The court viewed the matter as turning on what constituted appropriate proof that the telegraph contained the contractual authority. The court stated that telegraphic communications were to be treated like other writings, noting that the telegram had to be in written form at each end of the line and that it was appropriate to enter into evidence the original version of the message transmitted, or a copy thereof.[59]

A few years later, the New Hampshire Supreme Court decided *Howley v. Whipple*,[60] in which the court determined whether a telegraphed message complied with the Statute of Frauds. The court, in colorful and oft-cited language, held:

> [I]t makes no difference whether [the telegraph] operator writes the offer or the acceptance in the presence of his principal and by his express direction, with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by the use of the finger resting upon the pen; nor does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office.[61]

Over the remainder of the nineteenth century, courts almost routinely held that telegrams were writings within the meaning of the Statute of Frauds.[62]

The harder question with respect to whether a telegram satisfied the Statute of Frauds is whether it was signed by the sender. Early cases held them to be signed,[63] but the precedential effect of these cases was limited. During this pre-telephone era, the sender of a telegram went to the telegraph office, wrote out and signed the message, gave the written message to the telegraph operator, and the telegraph

---

57. 8 THE NEW ENCYCLOPAEDIA BRITANNICA 340, 340-41 (15th ed. 1995).

58. 29 Vt. 48 (1856).

59. *Id.* at 53; *see also* Trevor v. Wood, 36 N.Y. 307, 310-11 (1867) (telegraph medium plus a confirmatory letter is a sufficient writing).

60. 48 N.H. 487 (1869).

61. *Id.* at 488.

62. *See, e.g.*, Brewer v. Horst-Lachmund Co., 60 P. 418, 419 (Cal. 1900) (two telegrams read together constitute a note or memorandum); Smith v. Easton, 54 Md. 138, 146-47 (1880) (telegraphic dispatch is a writing); Western Twine Co. v. Wright, 78 N.W. 942, 944 (S.D. 1899) (copy of original telegram is a sufficient writing).

63. *E.g.*, *Howley*, 48 N.H. at 490.

company routinely kept the handwritten originals.[64] Hence, there was usually a paper version of the telegraphed message which the sender had manually signed in ink.

Even after the invention of the telephone, which allowed a sender to call the telegraph company and dictate a message to an operator who then transmitted it, courts eventually held that the telegram was signed. In *Selma Savings Bank v. Webster County Bank*[65] the court reasoned that sending a telegram in this manner was no different from dictating a message to one's secretary who would sign it and deliver the written message to the telegraph company for transmission.[66]

The modern view is illustrated by *Yaggy v. B.V.D. Co.*[67] where a seller of real estate sent a telegraphic acceptance of a buyer's offer and later failed to perform the contract. When sued by the buyer, the seller denied the existence of a contract, using the Statute of Frauds as a defense.[68] The court noted that printed letters had been held to satisfy the Statute of Frauds; therefore, the typewritten name of the seller at the end of the telegram was a sufficient signing so long as the seller directed the affixing of it with the intent to identify the telegram.[69]

Nevertheless, occasional decisions have cast doubt on whether a telegram can constitute a signed writing. For example, in *Pike Industries v. Middlebury Associates*[70] the court held that a telegraph message containing an indemnity agreement was not signed and thus did not satisfy the Statute of Frauds. The court stated:

> In this case there has been introduced no such signed document. The telegram contains no actual signature. The evidence does not disclose whether it was dispatched by telephone, or by submission of a written text. If the latter, no signed version has been introduced, if one exists, nor any signed authority of the sending agent. Therefore the Statute of Frauds bars use of the telegram as written evidence of an indemnity contract, and we so hold.[71]

---

64. Morrisson, *supra* note 9, at 647.

65. 206 S.W. 870 (Ky. 1918).

66. *Id.* at 872.

67. 173 S.E.2d 496 (N.C. Ct. App. 1970).

68. *Id.* at 501.

69. *Id*; *accord* Hillstrom v. Gosnay, 614 P.2d 466, 469 (Mont. 1980) (typewritten name in telegram is sufficient so long as it was affixed with intent to authenticate); Hansen v. Hill, 340 N.W.2d 8, 12 (Neb. 1983) (telegraph company acted as an agent of sender for purposes of signing); La Mar Hosiery Mills, Inc. v. Credit & Commodity Corp., 216 N.Y.S.2d 186, 190 (City Ct. 1961) ("any other view would be unrealistic and would produce pernicious consequences, impeding the conduct of business transactions"); *see also* Schneider v. Norris, 105 Eng. Rep. 388 (K.B. 1814) (holding that a printed name recognized as a signature constitutes a signing).

70. 398 A.2d 280, 282 (Vt. 1979).

71. *Id.* at 282.

The court did not cite to any of the multitude of prior cases holding that the sender's typewritten name appearing on the telegram constituted a sufficient signing.[72] Despite such rare and aberrational decisions, by the mid-twentieth century there was little doubt in most states that a telegram would satisfy both the writing and signing requirements of the Statute of Frauds.[73]

2. The Telex or Telecopier

In the twentieth century, the telegram gradually gave way to the telex machine, which allowed "each user to have direct access to every other user with a" similar machine,[74] without the need of the telegraph company as intermediary. The validity of agreements formed by telex under the Statute of Frauds was established in *Joseph Denunzio Fruit Co. v. Crane,*[75] where the court stated:

> [We] must take a realistic view of modern business practices, and can probably take judicial notice of the extensive use to which the teletype machine is being used today among business firms, particularly brokers, in the expeditious transmission of typewritten messages. No case in point has been called to the court's attention on this particular point, and a diligent search of the authorities has failed to uncover the status of teletype machines as satisfying the California Statute of Frauds. The point appears to be a res nova, but this court will hold that the teletype messages in this case satisfied the Statute of Frauds in California.[76]

Although no subsequent case has contained any extended discussion of the issue, later cases are consistent with the *Denunzio* court's holding that a telex is a signed writing.[77]

---

72. *See infra* note 73.

73. *See* Bartlett-Heard Land & Cattle Co. v. Harris, 238 P. 327, 329 (Ariz. 1925); Heffernan v. Keith, 127 So. 2d 903, 904 (Fla. Dist. Ct. App. 1961); Blackburn v. City of Paducah, 441 S.W.2d 395, 397 (Ky. Ct. App. 1969); *Hillstrom*, 614 P.2d at 470; *Hansen*, 340 N.W.2d at 12 ; J.E. Tarbell Co. v. Grimes, 149 A. 73, 75 (N.H. 1930); *La Mar*, 216 N.Y.S.2d at 190; Yaggy v. B.V.D. Co., 173 S.E.2d 496, 501 (N.C. Ct. App. 1970). *See generally* 2 ARTHUR LINTON CORBIN, CORBIN ON CONTRACTS § 522 (1950) (describing form of signature required); Morrisson, *supra* note 9, at 654 (concluding that law today requires a fact-based inquiry into the subjective intent of the sender).

74. Richard Allan Horning, *Has Hal Signed a Contract: The Statute of Frauds in Cyberspace*, 12 SANTA CLARA COMPUTER & HIGH TECH. L.J. 253, 286 (1996).

75. 79 F. Supp. 117 (S.D. Cal. 1948), *motion for new trial granted*, 89 F. Supp. 962 (S.D. Cal. 1950), *rev'd on other grounds*, 188 F.2d 569 (9th Cir. 1951).

76. *Id.* at 128-29.

77. *See, e.g.*, Apex Oil Co. v. Vanguard Oil & Serv. Co., 760 F.2d 417, 423 (2d Cir. 1985) (stating that the telex confirming Apex's obligation to purchase satisfied the written confirmation exception in U.C.C. § 2-201(2)); Interocean Shipping Co. v. National Shipping & Trading Corp., 523 F.2d 527, 537-38 (2d Cir. 1975) (holding that a telex evidencing the guarantee and signed by the agent of the party to be charged satisfies the Statute of Frauds).

3. *The Telefacsimile (Fax) Machine*

Given the greatly increased use of fax machines in recent years, it is surprising that there are no reported cases deciding whether a fax transmission constitutes a sufficient writing for purposes of the Statute of Frauds [78], although one court clearly assumed that it does. In *Bazak International Corp. v. Mast Industries*[79] the court held that five telecopied[80] purchase orders constituted confirmations that satisfied the requirements of section 2-201(2) of the U.C.C.[81] The court, however, did not specifically address the question of whether a fax message was a writing, and the parties apparently did not raise the issue.[82]

A court addressed whether a fax is signed in *Parma Tile Mosaic & Marble Co. v. Estate of Short*[83] where a contractor faxed a message to the plaintiff stating that it would be willing to guarantee payment for goods delivered to a subcontractor. The fax machine had been programmed to print the contractor's name at the top of the page, but no manual signature appeared at the bottom of the page.[84] In a subsequent dispute, the contractor claimed that the Statute of Frauds barred enforcement of the promise because there was no subscription as required by the relevant Statute of Frauds.[85] The trial court rejected this contention and, citing *Bazak*, held that the signature does not have to be in ink at the bottom of the page, but could be any symbol whether written or printed, appearing on any part of the document.[86] The trial court also concluded that the contractor "should not be permitted to evade its obligation because of the current and extensive use of

---

78. The effect of a fax transmission has been litigated with respect to questions other than the Statute of Frauds. For example, in *American Multimedia, Inc. v. Dalton Packaging Inc.*, 540 N.Y.S.2d 410, 412 (Sup. Ct. 1989), the court assumed that a faxed purchase order containing an arbitration clause was a writing for purposes of a federal arbitration statute. In *Calabrese v. Springer Personnel*, 534 N.Y.S.2d 83, 83 (Civ. Ct. 1988), the defendant received a faxed copy of an order to answer plaintiff's interrogatories. When the defendant failed to submit the answers within the time specified by the order, the plaintiff moved for sanctions. The issue turned on whether the defendant had been served. The court ruled that the faxed order clearly satisfied the plain intent of the rule governing service of papers. *Id.* at 84.

79. 538 N.Y.S.2d 503 (1989).

80. *Id.* at 509. Although the court used the term "telecopied," which is usually synonymous with a telex, the court's description of the documents involved suggests that the method of transmittal was a fax machine.

81. *Id.*

82. The court must have assumed, without deciding, that the faxed messages were writings, because in order for a message to qualify as a "confirmation" it must be "sufficient against the sender." U.C.C. § 2-201(2) (1995). To be sufficient against the sender, it must satisfy the requirements of section 2-201(1), which includes a "*writing* sufficient to indicate that a contract for sale has been made between the parties." *Id.* § 2-201(1) (emphasis added).

83. 590 N.Y.S.2d 1019 (Sup. Ct. 1992), *aff'd mem.*, 619 N.Y.S.2d 628 (App. Div. 1994), *rev'd*, 663 N.E.2d 633 (1996).

84. *Id.* at 1020.

85. *Id.*

86. *Id.*

electronic transmissions in modern business transactions."[87]

On appeal, however, the New York Court of Appeals reversed. It stated that a name is not a signature "'unless inserted or adopted with an intent, actual or apparent, to authenticate a writing.'"[88] The court said that no intent to authenticate resulted merely from the machine-generated name at the top of the page, and that no such intent could be inferred from the act of programming the fax machine to print the name: "We also reject plaintiff's contention that the intentional act of programming a fax machine, by itself, sufficiently demonstrates to the recipient the sender's apparent intention to authenticate every document subsequently faxed."[89] Although the Court of Appeals held that the particular fax did not satisfy the Statute of Frauds, nothing in the opinion suggests that a fax is not a writing or that it could not be signed if it bore some human-generated symbol constituting a signing.

Another recent decision casts more doubt on whether a fax constitutes a signed writing. In *Department of Transportation v. Norris*[90] a Georgia statute required that a claimant provide written notice to the Department within one year of the date of injury as a prerequisite to filing suit. Claimant sent a fax transmission to the Department, which it received within the one-year period, but a subsequent written notice was received after the expiration of the period. The court held that the fax transmission was not given in writing and observed:

> It may also be added that a facsimile transmission does not satisfy the statutory requirement that notice be "given in writing." Such a transmission is an audio signal via a telephone line containing information from which a writing may be accurately duplicated, but the transmission of beeps and chirps along a telephone line is not a writing, as that term is customarily used. Indeed, the facsimile transmission may be created, transmitted, received, stored and read without a writing, in the conventional sense, or hard copy in the technical vernacular, having ever been created.[91]

On appeal, the Georgia Supreme Court reversed, holding that the mailing of the written notice satisfied the statutory requirement that the notice be presented to or given within one year even though it was not received until after the expiration of the one-year period and, thus, the court did not address the sufficiency of the faxed notice.[92] However, the dissenting opinion concluded that the facsimile transmission failed to satisfy the writing requirement of the statute, stating that "[the legislature]

---

87. *Id.* at 1021.

88. *Parma Tile*, 663 N.E.2d at 635 (quoting Mesibov, Glinert & Levy v. Cohen Bros. Mfg. Co., 157 N.E. 148, 149 (Ct. App. 1927)).

89. *Id.*

90. 474 S.E.2d 216 (Ga. Ct. App. 1996), *rev'd sub nom.* Norris v. Georgia Dep't of Transp., 486 S.E.2d 826 (1997).

91. *Id.* at 218.

92. *Norris*, 486 S.E.2d at 827, 828 n.1.

did not see fit to include facsimile transmission as an appropriate method for presenting written notification."[93] Although *Norris* did not involve the Statute of Frauds or the issue of contract formation or validity, the case does indicate that a court may well determine that the concept of a writing is not broad enough to include information that is transmitted electronically, even if it is reproduced on paper by the recipient of the transmission.

4. Tape Recordings

A few cases have addressed the issue of whether an audiotape of a conversation, during which a contract is formed or acknowledged, satisfies the Statute of Frauds. A leading case is *Ellis Canning Co. v. Bernstein*,[94] involving a contract to sell corporate shares. The parties had taped a telephone conversation of their agreement in anticipation of a later final written agreement. Although the court held that there were sufficient, subsequent written documents to satisfy the Statute of Frauds contained in section 8-319 of the U.C.C.,[95] the court went on to address whether the tape recorded conversation alone could satisfy the Statute:

> But we go a step farther, and we freely concede that the step we take is not supported by any reported case we have been able to find. We hold that when the parties agreed to the tape recording of the oral agreement, that tape recording satisfies the requirements of [section 8-319]. This conclusion we reach by taking into account the fact that "[t]he purpose of the statute is to prevent fraud and perjury in the enforcement of obligations depending for their evidence on the unassisted memory of witnesses."
>
> . . . .
>
> We think and we hold that when the parties to an oral contract agree that the oral contract shall be tape recorded, the contract is "reduced to tangible form" when it is placed on the tape. . . . So, we hold that even if the signed correspondence were insufficient to get around the statute [which it isn't], the tape recording of the oral contract would be a "reduction to tangible form" under the provisions of the U.C.C. Probably the opposite result would be required under historical statutes of frauds which do not contain the tangible form language of this somewhat unusual definition of the word "written." However, under this statute, we think that the tape recorded agreement meets its requirements.[96]

---

93. *Id.* at 829 (Hines, J., dissenting).

94. 348 F. Supp. 1212 (D. Colo. 1972).

95. *Id.* at 1228. The 1994 Revision of Article 8 repealed the prior writing requirement of section 8-319. *See* U.C.C. § 8-113 (1994) (making the Statute of Frauds inapplicable to securities transactions).

96. *Ellis*, 348 F. Supp. at 1228 (footnote omitted) (citation omitted). The U.C.C. provision discussed in the case defined the terms "written" or "writing" as a printing, typewriting, or any other intentional reduction to tangible form. *See* U.C.C. § 1-201(46) (1995). *Accord* Londono v. City of

However, two New York cases have held that tape recorded conversations do not satisfy the writing requirement of the Statute of Frauds. In *Sonders v. Roosevelt*[97] the court held, without discussion, that a recorded telephone conversation is not a note or memorandum in writing as required by the Statute of Frauds.[98] In *Roos v. Aloi*[99] the court, noting that it was bound by the decision in *Sonders*, held that a tape recorded conversation during which one stockholder promised to purchase the stock of another did not satisfy the Statute of Frauds.[100]

Even if a tape recording might be a writing for purposes of the Statute of Frauds, the more difficult issue is whether and how it could be signed. In *Ellis Canning Co.* the court, after concluding that the tape recorded telephone conversation constituted a writing, also held that under the circumstances, the requirement of a signing was also satisfied.[101] The court reasoned: "We do not overlook the requirement for signature contained in the statute, but the clear purpose of this is to require identification of the contracting party, and where, as here, the identity of the oral contractors is established, and, in fact, admitted, the tape itself is enough."[102]

However, in *Swink & Co. v. Carroll McEntee & McGinley, Inc.*[103] the court assumed that the tape recording could be an "intentional reduction to tangible form" and thus qualify as a writing,[104] but held that it did not comply with the requirement that it be "signed by . . . the party against whom enforcement is sought."[105]

5. *Computer Records and Other Writing Issues*

Although no court has yet determined whether a computer-stored or computer-generated record satisfies the Statute of Frauds, a few courts have equated computer records with writings for purposes of other statutes. For example, in *Clyburn v. Allstate Insurance Co.*[106] a South Carolina statute made cancellation of an insurance policy contingent on the insurer giving ten days written notice to the insured and to the agent of record.[107] The insurer sought to cancel the insured's policy and sent written notice to the insured and a computer disk containing the cancellation notice

---

Gainesville, 768 F.2d 1223, 1227 n.4 (11th Cir. 1985) (stating that a tape recording satisfies Statute of Frauds).

97. 476 N.Y.S.2d 331 (App. Div. 1984), *aff'd mem.*, 487 N.Y.S.2d 551, 552 (1985).

98. *Id.* at 331-32. Judge Kupferman dissented in part and opined that a tape recording is of such a permanent nature as to satisfy the purposes of the Statute. *Id.* at 332.

99. 487 N.Y.S.2d 637 (Sup. Ct. 1985).

100. *Id.* at 642-43.

101. *Ellis*, 348 F. Supp. at 1228.

102. *Id.*

103. 584 S.W.2d 393 (Ark. 1979).

104. *Id.* at 399.

105. *Id.*

106. 826 F. Supp. 955 (D.S.C. 1993).

107. *Id.* at 956.

to the agent. The court determined that the disk satisfied the statutory requirement of written notice.[108]

Similarly, in *Wilkens v. Iowa Insurance Commissioner*[109] a number of insurance agents sued an insurer for allegedly violating Iowa insurance law by having many of its policies countersigned by a computer-generated, typewritten signature of a single agent, thus depriving the plaintiffs of their commission for countersigning.[110] The Iowa statute in question required a signature, and the court held that the computer-generated signature satisfied this requirement.[111] The court stated:

> We find the fact that the signature is computer-generated rather than hand-signed does not defeat the purpose of the act. The issue is not how the name is placed on a sheet of paper; rather, the issue is whether the person whose name is affixed intends to be bound. No one argues that the agent whose name was affixed did not intend to be bound. We find the signature requirements of the statute were met.[112]

The plaintiffs also alleged that the insurer had failed to comply with an Iowa statute requiring insurers to keep "a written record of each transaction" subject to inspection by the Commissioner of Insurance, because the insurer kept the records in its computer system.[113] The court approved the Commissioner's determination that the insurer complied with the law and stated: "[The Iowa statute] originated in 1939. We recognize, as the commissioner argues, that methods of doing business have changed considerably since the time of the enactment of the statute. The advent of the computer age has resulted in businesses making substantial changes in record-keeping procedures."[114]

However, a recent federal case involving bankruptcy law is a cautionary note that courts are not ready to equate a computer-generated record with a writing for all purposes. In *In re Kaspar*[115] debtors applied for a line of credit and a credit card over the telephone.[116] In response to questions asked by the creditor's employee, they provided financial information which the creditor's employee entered into a computer. The debtors never saw the computer generated summary of information. The creditor then issued the line of credit and the credit card. When the debtors filed

---

108. *Id.* at 956-57.
109. 457 N.W.2d 1 (Iowa 1990).
110. *Id.* at 2.
111. *Id.* at 3.
112. *Id.*
113. *Id.*
114. *Id.* at 4; *see also* Colorado v. Avila, 770 P.2d 1330, 1332 (Colo. Ct. App. 1988) (computer disk is a written instrument for the purpose of the forgery statute); Illinois v. Rushton, 626 N.E.2d 1378, 1389 (Ill. App. Ct. 1993) (computer-generated blood alcohol test results satisfy the writing requirement of the criminal DUI statute).
115. Bellco First Fed. Credit Union v. Kaspar (*In re* Kaspar), 125 F.3d 1358 (10th Cir. 1997).
116. *Id.* at 1359.

for bankruptcy, the creditor sought an order declaring its debts nondischargeable based on misrepresentations made to it by the debtors. The bankruptcy court denied the order and found that the creditor had failed to meet its requirement of showing that the materially false statement was a "statement in writing" as required by § 523(a)(2)(B) of the Bankruptcy Code.[117] The court framed the question and its answer in this fashion:

> This appeal presents the question of whether modern technology and business practices grounded in convenience will prevail over the strict language of statutory law. In particular, we address whether a computer generated statement of financial condition given in an application for credit neither seen nor signed by the debtor constitutes "a writing" under § 523(a)(2)(B) of the Bankruptcy Code.... We believe the statute must be literally interpreted, and the oral statements made by the debtor which led to the computer generated form are not to be regarded as the functional equivalent of a "writing" within the meaning of § 523(a)(2)(B).[118]

The court based its decision on a number of considerations. First, the court cited authority that the writing had to be prepared by the bankrupt, signed by the bankrupt, or written by someone else, but adopted and used by the debtor.[119] Second, the court noted the ordinary rule that exceptions to discharge should be narrowly construed.[120] Third, the court noted that "giving a statement of financial condition is a solemn part of significant credit transactions; therefore, it is only natural that solemnity be sanctified by a document which the debtor either prepares or sees and adopts."[121] More significant, however, are observations the court made about the absence of a paper record:

> In a world where important decisions relating to the extensions of credit and service will be made upon the contents of a statement relating to financial condition, too much mischief can be done by either party to the transaction were it [not required that the writing be prepared or seen and adopted by the debtor]. Somewhere in the commercial risk allocation picture, the writing must stand as a bulwark which tends to protect both sides.
>
> A creditor who forsakes that protection, abandoning caution and sound business practices in the name of convenience, may find itself without

---

117. *Id.*; *see* 11 U.S.C. § 523(a)(2)(B) (1993).

118. *Kaspar*, 125 F.3d at 1359.

119. *Id.* at 1361 (citing 4 COLLIER ON BANKRUPTCY ¶ 523.08[2][a] (15th ed. rev. 1997)). *But see* Chevy Chase Fed. Sav. Bank v. Graham (*In re* Graham), 122 B.R. 447, 451 (Bankr. M.D. Fla. 1990).

120. *Kaspar*, 125 F.3d at 1361.

121. *Id.*

protection.[122]

To date, no reported case has addressed the issue whether a computer record is signed or how such a signing might occur.

6. Lessons from Cases Involving Earlier Technologies

The cases involving emerging technologies and the Statute of Frauds clearly send conflicting signals about the likelihood that courts will find that electronic commerce messages satisfy the current requirements of the Statute of Frauds. On the one hand, courts have generally been hesitant to invalidate transactions on Statute of Frauds grounds where the court was convinced that the use of the particular technology involved was widespread.[123] Likewise, courts have been willing to look to the reliability of the particular technology and hold it satisfies the Statute of Frauds if it is comparable to the reliability of handwritten, paper-based documents.[124] Finally, with respect to the requirement of a signature, courts have found that typewritten, printed symbols are the equivalent of a handwritten signature on telegrams[125] and telexes,[126] and have even held that a tape recording is signed if the voices thereon are identified and the parties admit the existence of the conversation.[127] Many commentators have concluded that electronic commerce messages would satisfy the requirements of the Statute of Frauds.[128]

---

122. *Id.*

123. *See, e.g.*, Joseph Denunzio Fruit Co. v. Crane, 79 F. Supp. 117, 128-29 (S.D. Cal. 1948) (telecopier); Parma Tile Mosaic & Marble Co. v. Estate of Short, 590 N.Y.S.2d 1019, 1021 (Sup. Ct. 1992), *aff'd mem.*, 619 N.Y.S.2d 628 (App. Div. 1994), *rev'd*, 663 N.E.2d 633 (1996) (facsimile transmission); La Mar Hosiery Mills, Inc. v. Credit & Commodity Corp., 216 N.Y.S.2d 186, 190 (City Ct. 1961) (telegram).

124. *See, e.g.*, Hessenthaler v. Farzin, 564 A.2d 990, 993-94 (Pa. 1989) (mailgram is a signed writing for purposes of Statute of Frauds). However, given that an electronic commerce transaction will not generate a paper record, this rationale may be less applicable to such transactions than to telegrams, telexes, or faxes, where the semipermanent nature of the machine-imprinted paper provides inherent indicia of reliability. *See supra* note 54 and accompanying text.

125. *See, e.g.*, Hillstrom v. Gosnay, 614 P.2d 466, 469 (Mont. 1980); Hansen v. Hill, 340 N.W.2d 8, 12 (Neb. 1983); *Hessenthaler*, 564 A.2d at 993.

126. *See Joseph Denunzio Fruit Co.*, 79 F. Supp. at 128-29.

127. *See* Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212, 1228 (D. Colo. 1972).

128. 4 CAROLINE N. BROWN, CORBIN ON CONTRACTS § 23.1, at 762-64 & n.11 (Joseph M. Perillo ed., 1997); FORD & BAUM, *supra* note 1, § 3.3, at 44 ("[T]he combination of judicial acceptance of new technology, the development of trade usage, and legislative and administrative enactments suggests that electronically formed agreements will be found to constitute enforceable contracts for most statute of frauds purposes."); Horning, *supra* note 74, at 299; Houston Putnam Lowry, *Does Computer Stored Data Constitute a Writing for the Purposes of the Statute of Frauds and the Statute of Wills?*, 9 RUTGERS COMPUTER & TECH. L.J. 93, 105-07 (1982); Robert W. McKeon, Jr., *Electronic Data Interchange: Uses and Legal Aspects in the Commercial Arena*, 12 J. MARSHALL J. COMPUTER & INFO. L. 511, 532-33 (1994) (EDI transactions); Morrison, *supra* note 9, at 662 (1992) (EDI transactions); John Robinson Thomas, Note, *Legal Responses to Commercial Transactions Employing Novel Communications Media*, 90 MICH. L. REV. 1145, 1159-60, 1164 (1992) (fax and e-mail

On the other hand, communication technologies of the past, with the exception of the tape recordings, have all involved the production of a paper-based written message as the final product, whether telegram, telex printout, or faxed document.[129] It is, therefore, not a great step from holding that a handwritten, paper document satisfies the Statute of Frauds to the conclusion that a typewritten version of a message transmitted electronically also satisfies the Statute of Frauds.

Electronic commerce messages, however, are not produced on paper. Indeed, one of the primary advantages of electronic commerce is that it is no longer necessary to retain paper documents to memorialize transactions.[130] It is, therefore, much harder for courts to conclude that electronic commerce messages are writings as required by the Statute of Frauds. In addition, even if a paper printout of the electronic message is produced, the difficult question of how such paper can be signed remains, particularly after the New York Court of Appeals decision in *Parma Tile*,[131] which held that machine-generated symbols do not constitute a signing for Statute of Frauds purposes.[132]

This difficulty is highlighted by the split of authority about whether a tape recording can constitute a writing.[133] One court has held that a tape recorded conversation was the equivalent of a writing, emphasizing the reliability of the evidence to establish the terms of the contract,[134] whereas two other cases have summarily held that a tape recording is not a note or memorandum required by the particular statute in question.[135] Furthermore, even if a tape recording might be a writing, because it does not result in a paper document, there is the possibility that courts will find that it is not signed.[136] Similarly, an electronic message that is not reprinted on paper presents the likelihood that courts may conclude that the message is not a signed writing.[137] Accordingly, there is a substantial likelihood that courts

---

transactions).

129. Modern variations on the telex and fax allow for the message to be stored in a receiving computer terminal, rather than being printed on paper, but none of the reported cases approving these technologies involved such an arrangement.

130. *See* WRIGHT, *supra* note 6, § 2.4, at 2:6-:7.

131. 590 N.Y.S.2d 1019 (Sup. Ct. 1992), *aff'd mem.*, 619 N.Y.S.2d 628 (App. Div. 1994), *rev'd*, 663 N.E.2d 633, 635 (1996).

132. *See supra* notes 88-89 and accompanying text.

133. *See supra* notes 94-105 and accompanying text.

134. *See* Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212, 1228 (D. Colo. 1972).

135. Roos v. Aloi, 487 N.Y.S.2d 637 (Sup. Ct. 1985); Sonders v. Roosevelt, 476 N.Y.S.2d 331 (App. Div. 1984), *aff'd mem.*, 487 N.Y.S.2d 551 (1985).

136. *See* Swink & Co. v. Carroll McEntee & McGinley, Inc., 584 S.W.2d 393, 399 (Ark. 1979).

137. Of course, it is usually possible to print out a paper copy of the electronic message once a party has denied the existence of the contract and argue that the paper printout satisfies the Statute of Frauds. Normally, the memorandum need not be created contemporaneously with the formation of the agreement to satisfy the Statute of Frauds. 2 CORBIN, *supra* note 73, § 503, at 714-15. However, if the memorandum is prepared and filed after the initiation of a legal proceeding, it may be too late for the enforcement of the contract in that proceeding. *Id.* § 503, at 715 (authorities cited). *But see* 4 BROWN, *supra* note 128, § 22.8, at 744 ("There is good evidence that the old rule disallowing memoranda made after the filing of a complaint has become an anachronism.").

may balk at finding that electronic messages satisfy the Statute of Frauds.

Even if courts should determine that electronic messages are sufficient to satisfy the Statute of Frauds, those determinations would occur on a case-by-case basis over a period of years. Given the existing reluctance of parties to engage in electronic commerce, it is unlikely that enough courts would decide that electronic messages satisfy the Statute of Frauds to give much comfort to business persons in the foreseeable future.[138] Therefore, it is essential that legislatures examine the relation of electronic commerce to the Statute of Frauds. This Article next evaluates the two alternatives—repeal or amendment of the Statute of Frauds—that legislatures are faced with in this area.

B. Repeal the Statute of Frauds

Although commentators have long advocated repeal of the Statute of Frauds,[139] and despite its repeal in England[140] and its omission from the United Nations Convention on the International Sale of Goods,[141] the practical likelihood of complete repeal of the Statute of Frauds in the United States is nil for a number of reasons.

First, attempts to remove the writing requirement with respect to contracts for the sale of goods have met substantial opposition in the recent Article 2 amendment process. The Article 2 Drafting Committee has reversed its long-standing position favoring repeal of the Statute of Frauds in favor of keeping a Statute of Frauds requirement, albeit subject to several exceptions.[142] Second, the drafters of proposed Article 2B, dealing with licenses of information, have repeatedly reaffirmed the need for certain Statute of Frauds requirements.[143] The drafters explained:

> [T]he need for statute of frauds protection is greater in information contracts than in the sale of goods, however. This is true because of the

---

138. The history of the telegraph does not give much encouragement. It was forty or fifty years after the invention of the telegraph before a majority of state courts had affirmed that a telegram could be a writing satisfying the Statute of Frauds and, as late as 1979, a state court held that a telegram did not satisfy the Statute of Frauds because it was not signed. *See* Pike Indus. v. Middlebury Assocs., 398 A.2d 280, 282 (Vt. 1979).

139. *See supra* sources cited in note 2.

140. Law Reform (Enforcement of Contracts) Act, 1954, 2 & 3 Eliz. 2, ch. 34 (Eng.). The statute retained the writing requirement for suretyship and land sale contracts.

141. United Nations Convention on Contracts for the International Sale of Goods, April 11, 1980, art. 11, 19 I.L.M. 668, 674 (entered into force Jan. 1, 1988).

142. U.C.C. § 2-201 (Discussion Draft Apr. 14, 1997). This draft, accompanied by a memorandum from the Reporter, Professor Richard E. Speidel, was submitted for discussion at the 74th Annual Meeting of the American Law Institute. At that meeting, a motion to repeal section 2-201's writing requirement was defeated by a vote of 143 to 78. *Actions Taken with Respect to Drafts Submitted at 1997 Annual Meeting* (visited May 3, 1998) <http://www.ali.org/ali/AMACTION.HTM>.

143. *See* U.C.C. § 2B-201 (Proposed Discussion Draft Nov. 1, 1997) (requiring a record authenticated by the party against which enforcement is sought).

> character of the subject matter, the threat of infringement, and the split interests involved in a license with ownership of intellectual property rights vesting in one party while rights to use or possess a copy of the intangible may vest in another party. These considerations buttress other arguments against repeal which include primarily the idea that the fraudulent practices and unfounded claims that this rule prevents justify the cost and that the statute codifies and encourages what might be regarded as desirable business practice.[144]

Third, no state has entirely repealed the Statute of Frauds.

These developments indicate that there is something deeply ingrained in the American commercial legal culture that adheres to the requirement of a writing (or its electronic equivalent), making repeal of the Statute of Frauds unlikely. In addition to these impediments to repeal the Statute of Frauds, there are also compelling policy reasons why it should be retained, in some revised form, with respect to electronic commerce. In order to understand why, it is necessary to review some of the principal arguments surrounding the purposes and effects of the Statute of Frauds as well as the arguments frequently advanced to support its repeal.

1. The Functions of Form and the Requirement of a Signed Writing

Although the prevention of perjured testimony of oral promises justified the original Statute of Frauds,[145] modern commentators have correctly pointed out that the Statute's formal requirements serve many purposes. In the most thoughtful work on this subject, Professor Joseph Perillo has explained that formal requirements generally can serve nine distinguishable functions in the law of contracts.[146] Professor Perillo concluded that the Statute of Frauds, as one type of formal requirement, served two of these functions reasonably well, three of the functions only modestly, and four of the functions only in rare circumstances or not at all.[147]

Professor Perillo stated that "the Statute of Frauds serves the psychological and

---

144. *Id.* reporter's note 1.

145. Willis, *supra* note 2, at 429. The reasons giving rise to this perceived need are generally described as the seventeenth century's uncontrolled discretion of juries, the rule prohibiting testimony by interested parties or their families, and the general lack of development of contract law during this period. *Id.* at 429-31. This familiar litany of reasons behind the Statute is traceable to Sir William Holdsworth. *See* 6 WILLIAM HOLDSWORTH, A HISTORY OF ENGLISH LAW 387-93 (Methuen & Co. Ltd. and Sweet & Maxwell Ltd. 1971) (2d ed. 1937) (relating the Statute of Frauds to the legal atmosphere of the seventeenth century).

146. Joseph M. Perillo, *The Statute of Frauds in the Light of the Functions and Dysfunctions of Form*, 43 FORDHAM L. REV. 39, 43-69 (1974). He denominated the functions as the psychological, earmarking and classifying, cautionary, clarifying, managerial, publicity, educational, regulatory and taxation, and evidentiary functions. *Id.*

147. *Id.* at 69-70.

evidentiary functions of form reasonably well."[148] He described the psychological function (sometimes referred to as the magical or sacramental function) as "impress[ing] upon the psyches of the contracting parties the rightfulness of fulfilling their promises even if subsequently they appeared disadvantageous."[149] He noted that the psychological effects of "putting the transaction in writing should not be minimized," even in the contemporary world.[150]

Professor Perillo described the evidentiary function as supplying and preserving evidence of a contract.[151] He noted that other methods, such as the requirement of disinterested witnesses, would serve the same function, but not as well as the writing requirement, which does not die and cannot be suborned.[152] Today, the evidentiary function is probably the dominant justification for the Statute of Frauds.

Professor Perillo concluded that the Statute of Frauds only modestly serves the purposes he described as earmarking, cautionary, and classifying functions.[153] The earmarking function contemplates the determination of that point in time at which the parties have passed beyond negotiations and have entered into an enforceable promise.[154] He noted that the mere existence of a signed writing does not eliminate uncertainty as to whether the parties have left the negotiation stage and that it does not insure enforceability because there are additional requirements for enforceability, principally the requirement of consideration.[155]

The cautionary function reminds the parties that they are entering into a legally enforceable arrangement which may have certain consequences.[156] Professor Perillo concluded that "the Statute of Frauds has influenced the habits of the nation by encouraging the reduction of contracts to writing," and has thus had some cautionary effect.[157] However, he also pointed out that it does not consistently serve this purpose, as illustrated by judicial decisions holding that a letter containing a repudiation of an earlier oral agreement may satisfy the Statute of Frauds.[158]

Finally, Professor Perillo described the classifying function as allowing the party dealing with the paper quickly to recognize that he is faced with a particular type of legal obligation.[159] He concluded that the Statute "neither directly nor indirectly encourages" this function.[160]

---

148. *Id.*
149. *Id.* at 45.
150. *Id.* at 47-48.
151. *Id.* at 64.
152. Perillo, *supra* note 146, at 68.
153. *Id.* at 69.
154. *Id.* at 48-49.
155. *Id.* at 50.
156. *Id.* at 53.
157. *Id.* at 56.
158. Perillo, *supra* note 146, at 56.
159. *Id.* at 51. This is typically applicable to negotiable instruments, where the form requirements of negotiability allow the prospective purchaser of commercial paper to determine whether the instrument is negotiable or not. *Id.*
160. *Id.* at 51-52. Professor Perillo noted that, except for serving "the regulatory function only in

2. *The Dysfunction of Form and the Requirement of a Signed Writing*

As Professor Perillo has noted, the functions of the Statute of Frauds must be examined in light of its dysfunctions. Perillo categorized the dysfunctions into three general objections: (1) it inhibits the "sovereignty of the individual will," (2) it is "inconvenient and slow[s] the pace of business," and (3) failure to comply with it "permits a party to renege on his pledged word, thereby defeating the justified expectations."[161] He dismissed the first objection, noting that the common law has never recognized the sovereignty of the individual will as a contract principle.[162] Professor Perillo also dismissed the second objection, noting that, for reasons independent of the Statute of Frauds, "modern business tends to reduce its commitments to writing."[163] In addition, he noted that this objection might have more force with respect to more cumbersome formal requirements, such as a seal or notarization, but it has little force where the Statute of Frauds requires only a written memorial of an agreement.[164] In contrast, Professor Perillo found the third objection both serious and vital. When form requirements allow one party to renege on his agreement, this may defeat the expectations of the other party, undermine the utility of promissory exchanges, and unduly favor the party with more ready access to legal advice.[165]

3. *Electronic Commerce and the Functions and Dysfunctions of Form*

Using Professor Perillo's categories as a framework for analysis, one can show that the formal requirements of the Statute of Frauds, if expanded to encompass some forms of electronic commerce, have even more utility and cause less

---

a special category," the Statute of Frauds does not serve the four remaining functions (regulatory, managerial, publicity, and educational) of formal contract requirements. *Id.* at 69. The managerial function, the desire of management to control the subordinates' actions through the use of prescribed forms, is not served by the Statute of Frauds because it focuses on private rights and is not concerned with relationships within private or public enterprises. *See id.* at 58-59. The publicity function, which informs the public of a transaction, is typically associated with the recording of security interests in real or personal property and is not served by the Statute because it does not require the public filing of contracts. *Id.* at 59-60. The educational function, which is typically associated with consumer-protection statutes such as the Truth in Lending Act, ordinarily mandates written disclosure of certain information in contracts. *Id.* at 60. This function is not served by the Statute. *Id.* at 62. Finally, the regulatory and taxation functions, normally designed to regulate certain contracts or to impose a tax on certain transactions, are probably only indirectly served by the provision in many Statutes of Frauds regulating brokerage contracts, but not by any other provisions in the Statute of Frauds. *Id.* at 62-64.

161. *Id.* at 70.

162. *Id.*

163. Perillo, *supra* note 146, at 70.

164. *Id.* The objection has even less force with respect to Article 2 of the U.C.C.'s writing requirement, which only requires that a writing must: (1) indicate the existence of a contract for sale; (2) specify a quantity; and (3) be signed by the party against whom enforcement is sought. U.C.C. § 2-201 cmt. 1 (1995).

165. Perillo, *supra* note 146, at 70.

dysfunction in the case of electronic commerce than in other methods of forming agreements.

a. The Functions of Formal Requirements in Electronic Commerce

Virtually all Statute of Frauds functions would be served by the formal requirement that an agreement formed in an electronic commerce transaction is only enforceable if it is evidenced by an "authenticated electronic message." For immediate purposes, this term means an electronic message that is reliably attributable to a particular person.

The psychological function is served by the requirement that the sender of an electronic message in some way authenticate the message.[166] More importantly, however, the evidentiary function would also be served by the requirement of an authenticated electronic message. In electronic transactions, especially stranger-to-stranger transactions, there is very little likelihood that there will be any other evidence of the existence of an agreement such as prior oral conversations or letters. Indeed, in stranger-to-stranger transactions the sole evidence of an agreement will be the electronic messages transmitted by the parties. Because these transactions are between people with no prior dealings, and because the transactions are conducted without the production of a paper record, the messages themselves will be the only evidence that can possibly be introduced in the event that one person fails to perform. Therefore, the presence of an electronically-created record of the message would be the most likely and, in some cases, only evidence of the agreement.

Likewise, the requirement that the electronic message be authenticated by the person against whom the agreement is asserted would also serve the evidentiary function. Unlike the world of paper-based commerce, where the requirement of a signed writing most frequently serves the function of showing that an already-identified person made a particular promise, in the electronic commerce world, a requirement of an authenticated electronic message serves not only this function but the more fundamental function of identifying the person making the promise contained in the message in the first place. This additional function is critical in electronic commerce because there are few other methods of establishing the source of an electronic message. As mentioned earlier, it is very easy to spoof a receiving computer by impersonating another person with a different e-mail address.[167] Hence, the only way to begin to identify the source of a message is a requirement that the message bear some symbol or other mark that serves in some way to identify the sender.

166. *Id.* at 48.
167. *See* Oei, *supra* note 50, at 32.

b. The Dysfunctions of Form in Electronic Commerce

Of the three dysfunctions identified by Professor Perillo,[168] one is important in electronic transactions, and one is virtually meaningless in such transactions. First, the claimed dysfunction that formal requirements limit the scope of freedom of conduct makes as little sense in the electronic world as it does in the paper-based world.

However, the second claimed dysfunction—that formal requirements slow down the free flow of commerce—is a legitimate concern with respect to electronic transactions. To the extent that the Statute of Frauds requires the preservation of paper records of agreements, it is inconsistent with the emerging business practice of retaining only electronic records. Hence, unless the writing requirement is revised to validate at least some forms of electronic commerce, the Statute of Frauds will make business more expensive, less competitive, and less efficient by inhibiting the growth of electronic commerce. This has impelled the movement to reform the Statute of Frauds to accommodate electronic transactions. However, a different formal requirement, adapted to the practices of electronic commerce and freed of the paper requirement, would not likely slow down commerce.

The third dysfunctional aspect of formal contract requirements is preventing enforcement of agreements actually entered into without observing the formal requirements. As Perillo noted, this is a very powerful objection to the Statute of Frauds, because the absence of a writing satisfying the requirements of the Statute of Frauds can defeat justified expectations based on otherwise enforceable oral agreements.[169]

In the context of electronic commerce, however, this dysfunction of the Statute of Frauds simply does not apply. The premise of the argument of defeating expectations is that there is reliable evidence of a contract's existence through testimony of the existence of an oral agreement and that this testimony is excluded when the court rules as a matter of law that any agreement is unenforceable due to the absence of a writing. In other words, the absence of the required form prevents the proof of the substance of the transaction through other, presumably reliable, means.

With respect to open electronic commerce transactions,[170] particularly stranger-to-stranger transactions, there will ordinarily be no evidence of the agreement other than the electronic messages exchanged. Because the transactions will frequently be isolated transactions between persons with no history of dealing, the substance

168. Perillo, *supra* note 146, at 70.

169. *Id.*

170. With respect to EDI transactions, there will frequently be a master EDI agreement that provides some substantial basis for believing testimony about a subsequent transaction conducted pursuant to the master agreement. *See* The Electronic Messaging Services Task Force, *The Commercial Use of Electronic Data Interchange—A Report and Model Trading Partner Agreement*, 45 BUS. LAW. 1645, 1717-49 (1990) (proposing a model EDI master agreement).

of the transaction will be encompassed in the form of the messages exchanged. In other words, the difference between the form of the agreement and the substance of the agreement disappears with respect to most electronic commerce transactions. Hence, it makes perfect sense to continue the requirement of a form, an authenticated electronic message, to document these transactions. It is unlikely that the absence of the formal requirement will defeat the justified expectations of the parties unless a substantial destruction of the records of either the sender or the recipient occurs.[171]

Accordingly, the primary dysfunctional aspect of formal contract requirements does not apply with much force in the case of electronic transactions. Given that the evidentiary function of formal contract requirements is substantially advanced by requiring some authenticated electronic message, the case for revising the Statute of Frauds, rather than repealing it, is compelling.

C. Amend the Statute of Frauds to Validate Electronic Commerce

As demonstrated, the practical likelihood of a repeal of the Statute of Frauds is very small, and would not facilitate the proof of electronic commerce agreements. Instead, the focus of recent legislative developments has been to amend the Statute of Frauds in an attempt to validate electronic commerce transactions. Virtually all of the legislative developments have been at the state or uniform-law level. There has been little interest in federal legislation on the topic,[172] in part because of the current political climate and a recognition that premature national regulation may stifle the natural, evolving market forces which produce new models of electronic commerce that are both cost-efficient and reliable.[173] Furthermore, because electronic commerce is international in scope, there have been efforts at the international level to deal with the legality of electronic commerce transactions.[174]

---

171. Under the Statute of Frauds, the contract remains enforceable even though the writing is lost or destroyed, and the contents of the writing may be proven by parol testimony. 4 BROWN, *supra* note 128, § 23.10, at 827. One could reasonably assume that this doctrine would also apply to electronic messages that otherwise satisfy the Statute of Frauds.

172. An exception is the so-called "Baker Bill." Electronic Financial Services Efficiency Act of 1997, H.R. 2937 105th Cong., (1998) (section-by-section summary available at <http://www.house.gov/banking/hr2937ss.htm>). This bill establishes four criteria for electronic authentication to be valid and entitled to legal recognition. *Id.* § 6. It provides that any form of electronic authentication comporting with such standards "shall have standing equal to written signatures with respect to all communications with any agency or instrumentality of the United States government or with any U.S. Court." *Id.* § 5. It then provides: "Similarly, unless expressly prohibited by the laws of a state, any form of electronic communication that comports with the standards . . . , shall have standing equal to written signatures for purposes of any law." *Id.*

173. Information Security Committee, American Bar Ass'n, *States' Role in Developing Digital Signatures Policies and Standards* (July 31, 1997) <http://www.abanet.org/scitech/ec/isc/stateds.html>.

174. *See, e.g.*, *United Nations Commission on International Trade Law* (UNCITRAL) *Model Law on Electronic Commerce* (visited May 3, 1998) <http://www3.un.or.at/uncitral/texts/electcom/ml-ec.htm#TOP> (applying to all information used in

These international efforts have had substantial influence on the drafting of state laws.

This Article, however, focuses on uniform and state-law developments. These developments have involved two distinct issues: (1) equating electronic messages with signed writings for purposes of the Statute of Frauds; and (2) specifying consequences of the use of more secure forms of electronic communication as a method of proving that a particular individual in fact authored an electronic message. There has been remarkable agreement in legislation addressing the first of these issues, while the second of these issues has produced a wide variety of legislative responses. This portion of the article examines and analyzes these developments.[175]

1. *Legislative Efforts to Equate Electronic Records with Signed Writings*

All uniform legislation and most state legislation dealing with electronic commerce equates electronic messages with writings and makes provision for electronic messages being signed. The intended result is that an electronic message will satisfy the Statute of Frauds requirements of a writing that is signed. Although this result is nearly universal, the drafters of this legislation have used different, and sometimes confusing, terminology. Issues have also arisen about whether to exclude certain types of transactions from this legislation.

a. *The Uniform Commercial Code*

Electronic commerce issues have arisen in the drafting of revised Article 2 and proposed Article 2B of the U.C.C., as well as revised Article 2A on the leasing of goods. Presently, each of the three articles contains a Statute of Frauds provision.[176] The three drafting committees have coordinated their efforts with respect to electronic commerce issues and have now arrived at common definitions of critical terms used in the respective Statutes of Fraud. The critical development is the replacement of the existing concept of a "writing" that is "signed" with the concept of a "record" that is "authenticated."

Revised Articles 2 and 2A and proposed Article 2B use the term "record" as a substitute for the former requirement of a writing. Record is defined in Article 2B as: "information that is inscribed on a tangible medium, or stored in an electronic or other medium and retrievable in perceivable form."[177] This definition is designed

---

commercial activities).

175. In order to meet publication deadlines, this article only examines legislative developments through April 15, 1998.

176. U.C.C. § 2-201 (Annual Meeting Draft 1997); U.C.C. § 2A-201 (Annual Meeting Draft 1997); U.C.C. § 2B-201 (Proposed Draft Apr. 15, 1998).

177. U.C.C. § 2B-102(a)(38) (Proposed Draft Apr. 15, 1998).

to include those things that would currently constitute a writing under the U.C.C. as well as to encompass electronically stored information so long as it meets the "retrievable in perceivable form" requirement.

Revised Articles 2 and 2A and proposed Article 2B also use the term "authenticate" as a substitute for the former requirement that something be signed. Authenticate is defined as

> to sign, execute or adopt a symbol or sound, or encrypt or process a record in whole or part, with intent by the authenticating person to: (A) identify that person; (B) adopt or accept a record or term that contains the authentication or to which a record containing the authentication refers; or (C) attest to the integrity of a record or term that contains the authentication or to which a record containing the authentication refers.[178]

With these definitions of "authenticate" and "record", the drafters of revised Articles 2 and 2A and proposed Article 2B have simply provided that certain contracts for the sale or lease of goods or licenses of information must be evidenced by a "record authenticated by the party against which enforcement is sought."[179] Presently, Article 2B goes even farther and provides that "[a] record or authentication may not be denied legal effect, validity, or enforceability solely on the ground that it is in electronic form."[180] The purpose of this section is "to avoid any uncertainty about the efficacy of electronic records and signatures under state law as they apply to transactions covered by Article 2B."[181]

The most recent draft of proposed Article 2B has a series of "scope" sections that exclude certain transactions from coverage. Presently, the principal exclusion from coverage relates to agreements relating to core banking, payment, and financial services activities, including access to, use, transfer, clearance, settlement or processing of funds, instruments, or items.[182] In addition, proposed Article 2B also provides that its provisions are subject to any conflicting state statute or regulation that "establishes a consumer protection."[183]

---

178. U.C.C. § 2B-102(a)(3) (Proposed Draft Apr. 15, 1998). The current drafts of revised section 2-102(a)(1) of the Annual Meeting Draft 1997, and revised section 2A-102(a)(1) of the Annual Meeting Draft 1997, are slightly different. However, because the drafters of revised Articles 2 and 2A have simply incorporated subsequent developments in proposed Article 2B, one should anticipate that the definitions will ultimately conform exactly to that in Article 2B.

179. U.C.C. § 2B-201(a) (Proposed Draft Apr. 15, 1998); U.C.C. § 2-201(a), (Annual Meeting Draft 1997); U.C.C. § 2A-201(a) (Annual Meeting Draft 1997).

180. U.C.C. § 2B-113 (Proposed Draft Apr. 15, 1998).

181. U.C.C. § 2B-114, reporter's note (Proposed Draft Nov. 1, 1997). This provision is expected to become part of an electronic commerce package of sections that will ultimately be adopted in Articles 2 and 2A as well. *Id.*

182. U.C.C. § 2B-103A(4)(a)-(E) (Proposed Draft Apr. 15, 1998).

183. *Id.* § 2B-104(a)(2).

b. The Uniform Electronic Transactions Act

In 1996, the National Conference of Commissioners on Uniform State Laws appointed a committee to draft a new uniform act addressing questions of legally enforceable transactions consummated by electronic means. The drafting committee circulated three drafts of the Uniform Electronic Transactions Act (UETA) for comment.

The UETA reaches essentially the same result as the U.C.C., but uses slightly different terminology. The present draft of the proposed act defines an "electronic record" as "a record created, stored, generated, received, or communicated by electronic means."[184] The UETA then provides: "(a) A record may not be denied legal effect, validity or enforceability solely because it is an electronic record. (b) If a rule of law requires a record to be in writing, or provides consequences if it is not, an electronic record satisfies that rule."[185]

With respect to the requirement that a writing be signed, the current draft of the UETA defines "signature" as:

> any symbol, sound, process, or encryption of a record in whole or in part, executed or adopted by a person or the person's electronic agent with intent to: (A) identify that person; (B) adopt or accept a term or a record; or (C) establish the informational integrity of a record or term that contains the signature or to which a record containing the signature refers.[186]

An "electronic signature" is defined as "any signature in electronic form, attached to or logically associated with an electronic record."[187] The UETA then provides:

> A signature may not be denied legal effect, validity, or enforceability solely because it is in the form of an electronic signature.[188]

> If a rule of law requires a signature, or provides consequences in the absence of a signature, the rule of law is satisfied with respect to an electronic record if the electronic record includes an electronic signature.[189]

Hence, the UETA generally equates records with writings and validates electronic signatures for purposes of the Statute of Frauds.

---

184. UNIFORM ELECTRONIC TRANSACTIONS ACT § 102(7) (Discussion Draft Mar. 23, 1998) [hereinafter UETA]. A "record" is defined as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." *Id.* § 102(16).

185. *Id.* § 201(a), (b).

186. *Id.* § 102(20). The UETA defines "sign" as "to execute or adopt a signature." *Id.* § 102(19).

187. *Id.* § 102(8).

188. *Id.* § 301(a).

189. *Id.* § 301(b).

An earlier draft of the UETA contained a "scope" section that applied only to "any commercial or governmental transaction" that was intended by the drafters to exclude coverage of issues relating to the execution of wills and trusts.[190] However, the current draft of the UETA deletes the limitation to "commercial and governmental transaction"; instead, the drafters of the UETA have appointed a task force to draw up a list of excluded transactions.[191]

c. State Law Developments

About forty states have either enacted, or are considering, some form of legislation dealing with state-law requirements of signed writings in the electronic commerce context.[192] Two models have emerged with respect to whether electronic messages satisfy the Statute of Frauds. One is based on the landmark Utah Digital Signature Act.[193] The other model is broader in scope, with results similar to those under the uniform acts previously discussed.

(1) The Utah Model: Validating Only Electronic Messages with Digital Signatures

Utah adopted the Digital Signature Act in 1995.[194] The Utah statute was the first comprehensive attempt to conform the writing and signature requirements of the Statute of Frauds to the needs of electronic commerce and is the model for legislation adopted in Minnesota and Washington.[195] In order to understand the Utah statute, and others modeled on it, it is necessary to understand the concept of a "digital signature."

The use of digital signatures in electronic commerce is largely the result of efforts of the Information Security Committee of the American Bar Association's Section of Science and Technology (ISC). The ISC drafted the Digital Signature Guidelines in 1995 and revised them in 1996.[196] The Digital Signature Guidelines

---

190. UNIFORM ELECTRONIC TRANSACTIONS ACT §§ 103, 104, reporter's note 4 (Discussion Draft Nov. 1, 1997).

191. UETA, *supra* note 184, § 103, reporter's note 2.

192. A number of states have enacted statutes that simply allow certain forms of electronic records to be used by, or submitted to, branches of the state government. *E.g.*, ARIZ. REV. STAT. § 41-121 (1996) (allowing Secretary of State to approve "digital Signatures" for use by state agencies; 15 ILL COMP. STAT. 405/14.01 (1997) (allowing electronic signatures on communications between state agencies and the State Controller). Because these statutes do not deal with private transactions subject to the Statute of Frauds, this article will not discuss them.

193. UTAH CODE ANN. § 46-3-101 to -504 (Supp. 1997).

194. *Id.*

195. 1997 Minn. Laws § 325 K.001; WASH. REV. CODE § 19.34.010 (1997).

196. INFORMATION SECURITY COMMITTEE, AMERICAN BAR ASS'N, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE (1996) [hereinafter DIGITAL SIGNATURE GUIDELINES].

served as a model for the Utah statute.

A digital signature is not a version of a handwritten signature; instead, it is an encryption of the text of an electronic message which is appended to the message itself.[197] The digital signature is based on public key cryptography—the use of two codes (known as "keys") to send and receive messages. One of the keys, the "private" key, is kept solely in the possession of the sender of a message and is used to encode the text of the message into the digital signature.[198] Another key, the "public" key, is made publicly available to persons who may be dealing with the sender of the message. The public and private keys are mathematically related, but the relationship is so complicated that is "computationally infeasible" to deduce one key solely from knowledge of the other key.[199] Hence, the recipient of a message encrypted with the private key has ready access to the public key, but cannot deduce the private key from the public key.[200]

The keys are such that the digital signature created by one key can only be decrypted by the other key. Hence, a person receiving a digitally-signed document verified by use of the public key knows that a person possessing the private key sent the message.[201] The digital signature thus provides very reliable evidence of the source of an electronic message, assuming that the recipient has a reliable way of verifying the person with whom the private key is associated.

Verification of the person with whom the private key is associated is accomplished through the use of a trusted third party known as a "certification authority" or "CA."[202] The role of the CA is to verify the identity of a person possessing a key pair and then publish a "certificate"—an electronic record listing the public key as the subject of the certificate and confirming that the prospective signer identified in the certificate holds the corresponding private key.[203] This certificate is then made publicly available in a "repository"[204] maintained by the CA

---

197. More precisely, the electronic message is first condensed into a shorter form of digital representation, known as a "hash result," using an algorithm known as a "hash function." This hash result is then encrypted by the sender of the electronic message and it is the encrypted form of the hash result that is appended to the message. *Id.* at 9-12. This is known as the digital signature. *Id.* The reason for using the hash result is that the encryption uses such long numbers that there would be a tremendous drain on computing power if the entire message were encrypted. In order to be effective, hash functions must be truly "one-way"—it must be "computationally infeasible" to derive the text of the message which hashes to a given result. FORD & BAUM, *supra* note 1, § 4.3, at 115-16.

198. DIGITAL SIGNATURE GUIDELINES, *supra* note 196, at 10.

199. *Id.* at 10 n.23.

200. *Id.* at 10.

201. The recipient verifies the digital signature by taking the text of the electronic message and converting it into a hash result using the same hash function as the sender and then applying the public key to the hash result. The process results in verification only if the original message is encrypted by the use of a private key to which the public key is related. *Id.* at 12-13.

202. *Id.* at 17.

203. *Id.* at 17-18. For an exceptionally thoughtful preview of the likely issues raised by certification authorities and their activities, see A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. Rev. 49 (1996).

204. "Repositories" are online databases of certificates and other information available for

or someone else. A recipient of a digitally signed message will access the certificate and determine that a public key is associated with a private key possessed by a particular person, obtain a copy of that public key, and then use that public key to decrypt the digitally signed message the recipient received. By decrypting the digital signature, the public key exhibits extraordinarily reliable evidence that the message was in fact sent by a person in possession of the private key which the CA has verified as being associated with that public key.[205]

In addition to being a reliable method of identifying the source of an electronic message, a digital signature is also very good evidence that the message has not been tampered with since transmission. Because the digital signature is an encryption of the message itself, any alteration of a digitally signed message will cause the public key to fail to decrypt the digital signature, thus indicating to the recipient that the message has been altered since it was digitally signed.[206]

Hence, assuming that the CA has done an appropriate job of verifying the identity of the person associated with a public key (subscriber) and assuming that the subscriber has exercised reasonable care to prevent the loss or compromise of the private key, the use of digitally-signed messages provides an extraordinarily reliable method of validating both the source and the content of an electronic message.

Because of their reliability, digital signatures are the cornerstone of the Utah statute. Under the Utah statute, a digitally signed message satisfies both the requirement of a "writing" and a "signing" if the digital signature has been verified by reference to the public key listed in a valid certificate issued by a licensed CA.[207] The Utah statute provides that "[n]othing in this chapter precludes any symbol from being valid as a signature under other applicable law, including Uniform Commercial Code, Subsection 70A-1-201(39)."[208] Furthermore, "[n]othing in this chapter precludes any message, document, or record from being considered written or in writing under other applicable state law."[209] However, these provisions merely authorize courts to conclude that other forms of electronic messages may satisfy the requirements of a "signed writing." These provisions are not an affirmative legislative direction mandating this conclusion, as is the case under the uniform laws previously discussed. Accordingly, it remains unclear whether, in Utah, an electronic message that is not digitally signed can be considered either "written" or

---

retrieval and use in verifying digital signatures. DIGITAL SIGNATURE GUIDELINES, *supra* note 196, at 19.

205. The ability to identify a particular person as the source of an electronic message is frequently referred to as "signer authentication." *Id.* at 7-8.

206. *Id.* at 13.

207. UTAH CODE ANN. § 46-3-401, 403 (Supp. 1997). To qualify under the Utah statute, the digital signature must be affixed by the signer with the intent to sign the message. Also, the recipient cannot have notice that the signer has breached any duty it owes as a subscriber to the CA or that the signer does not rightfully hold the private key used to affix the digital signature. *Id.* § 401(1)(b), (c).

208. *Id.* § 401(2).

209. *Id.* § 403(2).

"signed."

(2) The Georgia Model: A Narrow Validation of Records with "Electronic Signatures"

Unlike the Utah statute, which is limited to digital signatures, the Georgia Electronic Records and Signatures Act[210] takes a seemingly broad approach to what types of electronic messages may satisfy the requirements of the Statute of Frauds. According to the Georgia act, when a person accepts or agrees to be bound by an "electronic record,"[211] any rule of law requiring a writing or signing shall be deemed satisfied if the record is "executed or adopted with an electronic signature."[212] The statute defines an "electronic signature" as a verification method that is "unique to the person using it, is capable of verification, is under the sole control of the person using it, and is linked to data [in the electronic message] in such a manner that if the data are changed the electronic signature is invalidated."[213] Hence, the act is not limited to digital signatures, but it is narrower than the terms "authentication" and "electronic signature" as used in the uniform acts. Because only records signed with an electronic signature satisfy the Statute of Frauds, the Georgia act would exclude any symbol that does not meet all four of the elements of an electronic signature. This effectively disqualifies any electronic message that is signed simply by name or other identifier, or that has not been appropriately linked to the electronic record.

(3) The Florida and Illinois Model: Open-Ended Validation Records with Electronic Signatures

In 1996, Florida enacted its Electronic Signature Act,[214] which takes a much broader approach than either Utah or Georgia. The Florida act states that, "[u]nless otherwise provided by law, an electronic signature may be used to sign a writing and shall have the same force and effect as a written signature."[215] The act defines "electronic signature" as "any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing."[216] The act then amends the existing statutory definition of "writing" to include "information which is created or stored in any electronic

210. GA. CODE ANN. §§ 10-12-1 to -5 (Supp. 1997).

211. A "record" is defined as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. 'Record' includes both electronic records and printed, typewritten, and tangible records." *Id.* § 10-12-3(2).

212. *Id.* § 10-12-4.

213. *Id.* § 10-12-3(1).

214. FLA. STAT. ANN. §§ 282.70 -.75 (West Supp. 1998).

215. *Id.* § 282.73.

216. *Id.* § 282.72(4). The act requires the electronic signature to be "logically associated" with such writing. *Id.*

medium and is retrievable in perceivable form."[217] Thus, the Florida act treats electronic messages identically to written messages for purposes of satisfying the Statute of Frauds.[218]

In April 1996, Illinois Attorney General Jim Ryan announced the formation of the Illinois Commission on Electronic Commerce and Crime, a task force formed to recommend legislation to the Illinois General Assembly that would encourage electronic commerce and provide safeguards from fraud and criminal activity involving electronic commerce. The Commission proposed the Illinois Electronic Commerce Security Act which has been introduced into the Illinois General Assembly.[219]

The proposed Illinois Act follows the Florida model by taking a very broad view of how electronic messages satisfy the requirements of a signed writing. It generally provides that an "electronic record"[220] satisfies any rule of law requiring information to be "written" or "in writing."[221] Furthermore, it states that an "electronic signature"[222] satisfies any rule of law requiring a signature.[223]

However, the proposed Illinois Act provides that electronic records with electronic signatures constitute neither a "writing" nor a "signing" in three cases. The first exception applies where treating an electronic record as a writing or an electronic signature as a signing would "involve a construction of a rule of law that is clearly inconsistent with the manifest intent of the lawmaking body or repugnant to the context of the same rule of law."[224] The second exception applies with respect " to any rule of law governing the creation or execution of a will or trust, living will, or healthcare power of attorney."[225] The final exception applies "to any record that

---

217. 1996 FLA. LAWS ch. 96-224, sec. 1.01(4).

218. The Act gives the Secretary of State the power to issue "certificates for the purpose of verifying digital signatures." FLA. STAT. ANN. § 282.74 (West Supp. 1998). Nonetheless, the Act specifically provides that a public or private entity does not have to participate in the Secretary of State's certification program to verify a digital signature. *Id.*

219. Electronic Commerce Security Act, H.R. 3180, 90th Gen. Assembly, 1997-1998 Reg. Sess. (Ill., introduced Feb. 11, 1998), *available at* (visited Apr. 28, 1998) <http://www.mbc.com/iecsa.html>.

220. The proposed Illinois Act defines "electronic record" as "a record generated, communicated, received, or stored by electronic means for use in an information system or for transmission from one information system to another," *id.* § 5-105, and "record" as "information that is inscribed, stored, or otherwise fixed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form." *Id.*

221. *Id.* § 5-115(a).

222. The proposed Illinois Act defines "electronic signature" as "a signature in electronic form attached to or logically associated with an electronic record," *id.* § 5-105, and "signature" as "any symbol executed or adopted, or any security procedure employed or adopted, using electronic means or otherwise, by or on behalf of a person with intent to authenticate a record." *Id.*

223. *Id.* §5-120(a).

224. *Id.* §§ 5-115(b)(1), 5-120(c)(1). The proposed Illinois Act also states that this exception does not apply simply because of the "mere requirement that information be 'in writing,' 'written,' or 'printed.'" *Id.*

225. Electronic Commerce Security Act §§ 5-115(b)(2), 5-120(c)(2), H.R. 3180, 90th Gen.

serves as a unique and transferable instrument of rights and obligations including, without limitation, negotiable instruments and other instruments of title wherein possession of the instrument is deemed to confer title."[226]

d. Analysis of the Various Models of Equating Electronic Records with Signed Writings

If electronic commerce is to be encouraged, it is necessary that electronic messages have legal validity equal to that of messages written on paper. All of the statutes described above move in this direction, but in varying degrees.

The Utah statute is too narrow because it limits electronic messages that satisfy the Statute of Frauds to those that are digitally signed. Unlike the Statute of Frauds, which can be satisfied by virtually any piece of paper bearing some symbol that tends to identify the defendant as a party to the contract,[227] the Utah statute requires a specific form of signature—a digital signature.[228] While this certainly advances the evidentiary function of the Statute of Frauds, it requires a level of reliability for electronic messages far beyond that required by the existing Statute of Frauds. This requirement could lead to the dysfunctional consequence of stifling a desirable form of commerce by requiring formalities inconsistent with the basic societal

---

Assembly, 1997-1998 Reg. Sess. (Ill., introduced Feb. 11, 1998), *available at* (visited Apr. 28, 1998) <http://www.mbc.com/iecsa.html>. The drafters believed that these types of documents require the formalism "of ceremony (including the need for counsel and due deliberation), or the attestation to sobriety and mental capacity and lack of obvious compulsion that is provided by third-party witnesses." Accordingly, the drafters concluded that until procedures are adopted to provide similar requirements for electronic records and signatures, these items should be excluded. *See id.* § 5-115, cmt. 7(b).

226. *Id.* §§ 5-115(b)(3), 5-120(c)(3). This exception was included because of the important rights associated with possession of an original negotiable instrument or document of title and the present inability to distinguish originals from copies in cases where information is sent and stored digitally. *Id.* § 5-115 cmt. 7(c). However, the proposed Illinois Act creates an exception to this exclusion from coverage if "an electronic version of such record is created, stored, and transferred in a manner that allows for the existence of only one unique, identifiable, and unalterable original with the functional attributes of an equivalent physical instrument, that can be possessed by only one person, and which cannot be copied except in a form that is readily identifiable as a copy." *Id.* §§ 5-115(b)(3), 5-120(c)(3). This exception was included to accommodate emerging technology that may provide for an identifiable and unalterable electronic record. *Id.* § 5-115 cmt. 7 (c).

227. *See, e.g.*, Zacharie v. Franklin, 37 U.S. 151, 162 (1838) (holding that a mark of "X" is a sufficient signature); Welch v. Mitchell, 351 So. 2d 911, 915 (Ala. Civ. App. 1977) (holding that a pre-printed name on bill of sale is a sufficient signature); Merrill, Lynch, Pierce, Fenner & Smith, Inc. v. Cole, 457 A.2d 656, 662-63 (Conn. 1983) (holding that a pre-printed name on confirmation slip is a sufficient signature); Kohlmeyer & Co. v. Bowen, 192 S.E.2d 400, 404 (Ga. Ct. App. 1972) (holding that letterhead is sufficient to authenticate a writing); Bains v. Piper, Jaffray & Hopwood, Inc., 497 N.W.2d 263, 271 (Minn. Ct. App. 1993) (holding that computer-generated letterhead satisfies the signature requirement); *see also* U.C.C. § 1-201(39) cmt. 39 (noting that a "signing" may be by initials or thumbprint). *But see* Parma Tile Mosaic & Marble Co. v. Estate of Short, 663 N.E.2d 633 (N.Y. 1996) (holding that a fax machine-generated name is not a sufficient signing).

228. UTAH CODE ANN. §§ 46-3-401, 403 (Supp. 1997).

expectations of the way transactions are to be consummated.[229] Indeed, the Utah statute is so narrow that even a person using software creating a digital signature might fail to satisfy the statute because of its narrow definitions relating to the use of digital signatures.[230]

Likewise, the Utah statute has been criticized for not being technologically neutral. Rather, it favors a specific technology—digital signatures—to the complete exclusion of other forms of electronic communication. This approach may have the effect of stifling the development and acceptance of existing or future technologies that might provide substantially equivalent assurance of the electronic message's authenticity and content.[231]

Like the Utah model, the Georgia model is under-inclusive. By requiring an "electronic signature" that satisfies the Statute of Frauds to be one that possesses the four statutory indicia of reliability, it requires much more of an electronic message than the current Statute of Frauds requires of a paper message. However, unlike Utah, the Georgia statute is technologically neutral, so that technologies other than digital signatures may qualify as an electronic signature. Unfortunately, the Georgia model does not specify a method for determining what types of other technologies may qualify as an electronic signature.

Presumably, the judiciary would decide the issue of a person using some other form of signing an electronic record and claiming that it qualifies as an "electronic signature." The likelihood of this actually occurring is small because someone would have to risk using new technology in a transaction involving a sum of money sufficient to justify litigation for the purpose of establishing an acceptable electronic signature. Hence, even though the Georgia statute may be technologically neutral,

---

229. When a required form . . . is regarded as an unnecessary bit of legalistic nonsense, it fails to serve a healthy psychological function. No matter what other functions the form may serve (evidentiary, cautionary, etc.), it becomes dysfunctional and will be discarded first by the persons subject to the law and then by the law itself.

Perillo, *supra* note 146, at 46.

230. WRIGHT, *supra* note 6, § 16.7.3, at 16:32. Mr. Wright posits three situations in which the digital signature requirements of the Utah statute would not be met. One involves the failure to utilize a "one-way function" as part of the encryption process. Another involves a third person who creates the one-way function, but another person who encrypts the function with his private key. The third involves the more likely scenario of a consumer using software that includes digital signature features, but having no idea how it works. Therefore, according to Mr. Wright, she would lack the statutorily-required intent to digitally sign the message. *Id.*

231. *Id.* § 16.7.3, at 16:31. For a comparison of the security risks of digital signatures and biometric identifiers, see R.R. Jueneman & R.J. Robertson, Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 JURIMETRICS J. (forthcoming Spring 1998). For example, biometric forms of identification, such as retinal scans or palm print scans, may in the future serve to identify the sender of a message. Likewise, the currently available PenOp technology digitizes biometric information about one's handwritten signature. According to its promoters, it can serve to identify the sender and unalterably affix the sender's signature to the electronic record. *See generally* Benjamin Wright, *Eggs in Baskets: Distributing the Risks of Electronic Signatures*, 15 J. MARSHALL COMPUTER & INFO. L. 189, 195-98 (1997) (summarizing PenOp technology).

its practical consequences may encourage parties to use digital signatures, the only current technology that clearly meets the definition of an electronic signature. Thus, this consequence retards the development and use of new forms of secure electronic communication.

A more appropriate alternative is one followed by Florida, Illinois, and the drafters of the uniform acts. This approach recognizes that because almost any scrap of paper bearing any symbol may constitute a signed writing for purposes of the Statute of Frauds, almost any electronic message bearing any form of identifying symbol may also constitute a "writing" that is "signed."

A final issue is the scope of the statutes designed to validate electronic messages as satisfying the Statute of Frauds. The drafters of revised Articles 2 and 2A and of proposed Article 2B of the U.C.C. enjoy the luxury of dealing with a single Statute of Frauds limited to the transactions within the scope of each Article. Therefore, they can amend the Statute of Frauds by using the broad terms "authenticate" and "record" without worrying about affecting other statutory requirements of a writing or a signing outside the scope of the Article.

However, neither the drafters of the UETA nor the various state legislatures could utilize this simple method to validate electronic commerce transactions. Instead, these drafters were required to draft generally applicable statutes equating electronic records with signed writings and to determine if the statute should exclude some state law requirements mandating information to be in writing or signed in transactions other than contracts subject to the Statute of Frauds.[232] Hence, questions abound whether some transactions should be excluded from the all-encompassing validation of electronic records and signatures.

Legislation has followed several different approaches. In Florida, the statute equates electronic records to signed writings in virtually all cases. Apparently, this statute encompasses documents that are not contract-based, such as wills, trusts, and powers of attorney, as well as negotiable instruments and other documents of title that involve the principle of negotiability and depend on the existence of a unique, transferable original.[233]

Despite the fact that all of these documents pose separate legal and practical issues from those presented by electronic contracts, the Florida statute appears to validate all electronic forms of such documents. The proposed Illinois Act takes the

---

232. Of course, it would be possible to identify each particular provision in a state code that requires a signed writing and amend each such provision by substituting "authenticated record" for "signed writing," but that would entail herculean effort and expense.

233. *See* FLA. STAT. ANN. § 282.73 (West Supp. 1998). The Georgia statute applies to persons who "accept or agree to be bound by an electronic record executed or adopted with an electronic signature." GA. CODE ANN. § 10-12-4 (Supp. 1997). Accordingly, one could argue that the Georgia statute only applies to transactions involving two persons, excluding from its scope wills, trusts, and other unilateral acts. However, the Georgia statute clearly encompasses negotiable instruments and documents of title, despite the conceptual difficulties associated with the concept of negotiability and electronic commerce. *See generally*, LARY LAWRENCE, AN INTRODUCTION TO PAYMENT SYSTEMS 34 (1997) (discussing the "signed" requirement for negotiability).

more cautious approach of excluding these transactions, as well as giving the court authority to exclude other transactions should the court find that the intent of the law covering transaction is inconsistent with the use of an electronic record. This approach avoids unintended consequences outside the contract area.

2. *Legislative Efforts Regarding Security Procedures Used to Verify the Source and Content of an Electronic Message*

Even if an electronic message can constitute a writing and even if it contains some electronic symbol or mark that renders it signed under the applicable Statute of Frauds, the party seeking to enforce a promise contained in an electronic message must prove that the record was signed by the opposing party. For transactions outside the Statute of Frauds the plaintiff must show that a promise was made by the defendant. So, how does one prove the identity of the sender of an electronic message?

Of course, a handwritten signature on a piece of paper can be verified as the defendant's signature by eyewitnesses who saw the defendant sign the paper, by comparison to other examples of the defendant's handwriting, by expert witness testimony based on similar comparisons, and by circumstantial evidence derived from the contents of the writing, indicating facts that only the defendant could know. However, in an electronic message, the symbol or other identifying mark that identifies the sender is a series of binary data that cannot be reliably associated with any particular individual. Absent eyewitness testimony (which would almost never be available), the recipient of an electronic message has a very difficult time proving who it.

Even if one can show that the defendant sent an electronic message, a second difficulty is proving that the electronic message introduced into evidence is the same message. A sender can always argue that, if the message was sent over an open network, a third person could have intercepted and altered it after it was sent and before it was received. Alternatively, the sender can argue that the recipient altered the information in the message after receipt. How, then, can the plaintiff prove that the defendant signed the precise message the plaintiff seeks to introduce at trial?

These arguments rarely arise in cases involving paper writings because of the semipermanent nature of ink on paper and the difficulty of secretly altering the content of the writing. However, these arguments are entirely plausible in an electronic environment, because digital information is malleable and can be changed in ways that are virtually impossible to detect.

The drafters of uniform legislation and state statutes relating to electronic commerce have confronted these issues. Unfortunately, the issue of "binding" an individual to an electronic message has led to many different and inconsistent approaches.

a. The Uniform Commercial Code

The drafters of proposed Article 2B[234] deal with this problem with the concept of an "attribution procedure" to verify the source and content of an electronic message. The drafters define an "attribution procedure" as: "a procedure established by law, regulation or agreement, or adopted by the parties for the purpose of verifying that an electronic authentication, record, message, or performance is that of the respective party or is for detecting changes or errors in content."[235]

An attribution procedure "may include algorithms, codes, identifying words or numbers, encryption, callback procedures, or any other reasonable security device."[236] If the attribution procedure is commercially reasonable,[237] the use of an attribution procedure can assist the recipient in proving the source of an electronic message. Under proposed section 2B-116, an electronic message is "attributable" to a person in two circumstances.[238] First, a message is "attributable" to a party if the message was in fact the action of the party or the party's agent.[239] Obviously,

---

234. The latest drafts of revised Articles 2 and 2A simply copied the then-current provisions of Article 2B. *See* U.C.C. §§ 2-210 to -214 (Discussion Draft 1997) (visited Jan. 28, 1998) <http://www.law.upenn.edu/library/ulc/ucc2/ucc2797.htm>; U.C.C. §§ 2A-207 to -212 (Discussion Draft 1997) (visited Jan. 28, 1998) <http://www.law.upenn.edu/library/ulc/ucc2/ucc2a797.htm>. Presumably, Articles 2 and 2A will conform to the electronic commerce provisions in the final draft of Article 2B. Accordingly, this article only discusses Article 2B with respect to these issues.

235. U.C.C. § 2B-115(a) (Proposed Draft Apr. 15, 1998).

236. *Id.* § 2B-114 reporter's note 3.

237. *Id.* § 2B-116(a)(2). "An attribution procedure established by law or regulation is commercially reasonable for the purposes for which it was established." *Id.* § 2B-114(1). As to attribution procedures agreed upon or adopted by the parties, commercial reasonableness "is determined in light of the purposes of the procedure and the commercial circumstances at the time the parties agree to or adopt the procedure." *Id.* § 2B-114(2). The question of commercial reasonableness of the attribution procedure is for the court. *Id.* §2B-114.

238. In addition to attribution, a person who has previously identified himself to others by use of numbers, codes, or computer programs may incur liability for losses caused by his negligence. The current draft of section 2B-116 provides:

> (c) A person is liable for losses in the nature of reliance, if the losses occur because:
>
> (1) the person failed to exercise reasonable care;
>
> (2) the relying person reasonably relied on the belief that the other person was the source of an electronic authentication, message, record, or performance;
>
> (3) that reliance resulted from acts of a third person that obtained access [to] numbers, codes, computer programs, or the like from a source under the control of the person that failed to exercise reasonable care; and
>
> (4) the use of the access numbers, codes, computer programs, or the like created the appearance that it came from that person.

Id. § 2B-116(c). The difficult issues relating to this loss-allocation scheme are beyond the scope of this article.

239. *Id.* § 2B-116(a)(1).

there is nothing remarkable about this alternative. If it can be established that a person, or the person's agent[240] sent a message, that person is responsible for it. The difficulty for the recipient, of course, is proving the identity of the sender when the purported sender denies responsibility for the message.

Second, an electronic message is "attributable" to a person if "the other person, in accordance with a commercially reasonable attribution procedure for identifying a person, in good faith reasonably concluded that it was the action of the other person, a person authorized by it, or the person's electronic agent."[241] This attribution method creates a presumption that the message is that of the party to whom it is attributed[242] and focuses on situations where the parties agree to use or adopt an attribution procedure.[243] The theory underlying this attribution method is that if the parties have agreed on a commercially reasonable method of identification, and if one party has used that method so as to indicate that the other party did send the message, then it is perfectly logical to create a presumption that the other party did, in fact, send the message. This presumption is rebuttable.[244]

The attribution rules of Article 2B also deal with the problem of establishing that the content of an electronic message has not been altered since it was transmitted. Section 2B-117 provides:

> If the parties use a commercially reasonable attribution procedure to detect errors or changes in the content of an electronic record, as between the parties, the following rules apply:

---

240. This section is innovative in that it approves the concept that a computer can be programmed to initiate or respond to a message without human intervention and that the act of that "electronic agent" is attributable to the principal. "Electronic agent" is defined as "a computer program or other electronic or automated means used, selected, or programmed by a party to initiate or respond on behalf of that person to electronic messages or performances in whole or in part without review by an individual." *Id.* § 2B-102(a)(18). *See generally* John P. Fischer, Note, *Computers as Agents: A Proposed Approach to Revised U.C.C. Article 2*, 72 IND. L.J. 545, 556-70 (1997) (analyzing the computer-principal agency relationship in proposed Article 2).

241. U.C.C. § 2B-116(a)(2) (Proposed Draft Apr. 15, 1998).

242. *Id.* § 2B-116(b).

243. *Id.* § 2B-116 reporter's note 3. One may assume that it also applies to an attribution procedure established by law.

244. *Id.* The U.C.C. provides that "presumption" or "presumed" means that "the trier of fact must find the existence of the fact presumed unless and until evidence is introduced which would support a finding of its non-existence." U.C.C. § 1-201(31) (1995). This is in accord with the rule in federal court and in most states that the effect of a presumption disappears if the other party introduces any evidence indicating the non-existence of the presumed fact. This is sometimes called the "bursting bubble" or "Thayer" approach. 9 JOHN HENRY WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW §§ 2490-91 (1981); KENNETH S. BROUN ET AL., MCCORMICK ON EVIDENCE § 344, at 582-83 (John William Strong ed., 4th ed. 1992). If the party against whom the presumption operates denies the existence of the presumed fact, then the presumption disappears. *Id.* A second, minority view is the "Morgan" or "burden shifting" approach which says that a presumption continues until the party against whom the presumption operates proves that it is more likely than not that the presumed fact did not occur. In other words, this latter view has the effect of shifting the burden of persuasion on the issue of the presumed fact to the person against whom the presumption operates. *Id.* at 586.

> (1) An electronic authentication, message, record, or performance that the attribution procedure shows to have been unaltered since a point in time is presumed to have been unaltered since that time.
>
> (2) An electronic authentication, message, record, or performance created or sent pursuant to the attribution procedure is presumed to have the content intended by the person creating or sending it as to portions to which the procedure applies.
>
> (3) If the sender complied with the attribution procedure, but the other party did not, and the change or error would have been detected had the other party also complied, the sender is not bound by the error or change.[245]

In effect, this section presumes that electronic records have not been altered or do not contain mistakes if the parties have used a commercially reasonable attribution procedure capable of detecting the same.[246]

b. The Uniform Electronic Transactions Act

With respect to electronic records and electronic signatures, the Uniform Electronic Transactions Act (UETA) defines a "security procedure" as:

> a procedure or methodology, established by law or regulation, or established by agreement, or adopted by the parties, for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the informational content of an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, callback or other acknowledgment procedures, or any other procedures that are reasonable under the circumstances.[247]

The UETA uses the concept of a security procedure to assist in establishing the identity of the sender of an electronic message in essentially the same way as Article 2B uses the concept of an attribution procedure. Section 202 of the UETA provides:

> (a) An electronic record is attributable to a person if . . . (2) the other person, in good faith and acting in compliance with a comercially

245. U.C.C. § 2B-117 (Proposed Draft Apr. 15, 1998).

246. Proposed Article 2B also provides for allocation of losses resulting from undetected errors including a novel provision that excuses consumers from being bound by errors in electronic messages not caused by the consumer's fault, so long as the consumer promptly notifies the other party of the error and does not retain any benefits of the transaction as a result. *Id.* § 2B-118.

247. UETA, *supra* note 184, § 102(18).

> reasonable security procedure for identifying the person to which the electronic record is sought to be attributed, reasonably concluded that it was the action of the other person, a person authorized by it, or the person's electronic agent. . . .
>
> (b) Attribution of an electronic record to a person under subsection (a)(2) has the effect provided for by the agreement regarding the security procedure and, in the absence of terms about such effect, creates a presumption that the electronic record was that of the person to which it is attributed.[248]

Thus the UETA creates a presumption of identity of the sender in basically the same circumstances as U.C.C. Article 2B.

In proving the integrity of the content of an electronic message, the UETA almost precisely tracks the approach of Article 2B. It provides:

> If the parties act in compliance with a commercially reasonable security procedure to detect errors or changes in the informational content of an electronic record, between the parties the following rules apply:
>
> (a) An electronic record that the security procedure shows to have been unaltered since a specified point in time is presumed to have been unaltered since that time.
>
> (b) An electronic record created or sent in accordance with the security procedure is presumed to have the informational content intended by the person creating or sending it as to portions of the informational content to which the security procedure applies.[249]

However, unlike Article 2B, the UETA provides for specific consequences of this presumption.[250] It states that "'[p]resumption' or 'presumed' means that the trier of fact must find the existence of the fact presumed unless and until evidence is introduced which would support a finding of its non-existence."[251] Thus the UETA adopts the "bursting bubble" approach to presumptions. Once the person against whom the presumption operates introduces any evidence that would support a finding of the nonexistence of the presumed fact, the mandatory effect of the presumption disappears.[252] Hence, with respect to the issue of the identity of the sender of the electronic message, if the person indicated by the security procedure

---

248. *Id.* § 202(a)(2), (b).

249. *Id.* § 203(a), (b).

250. *See supra* note 244.

251. UETA, *supra* note 184, § 102(15) [Alternative 1] (Discussion Draft Mar. 23, 1998). The present draft contains three alternative formulations of the definition, but each of them has the same substantive meaning. *Id.* reporter's note.

252. *See id.* reporter's note. The Reporter suggests that the drafting committee continue to consider whether the effect of the presumption should be specified. *Id.*

as the source of the message denies sending it, the mandatory effect of the presumption ceases and the issue of who sent the message becomes a question for the trier of fact. Similarly, if the sender of the message testifies that the content of the message is not the same as the one he sent, the mandatory effect of the presumption of message integrity also terminates, and a factual issue for the trier arises.

c. State Law Developments

Three substantially different approaches have emerged in state legislation concerning the issues of identifying the sender of an electronic message and establishing the integrity of the content of an electronic message. These approaches are the Utah approach, the Florida and Georgia approach, and the Illinois approach.

(1) The Utah Approach: Evidentiary Presumptions Based on Digital Signatures

As noted earlier, the Utah Digital Signature Act addresses only electronic records that are signed with a digital signature.[253] In addition, the statute provides that if the digital signature is verified by the public key listed in a valid certificate issued by a licensed CA, the court shall presume that the digital signature is that of the person listed in the certificate, that it was affixed by that person with the intention of signing the message, and that the recipient had no notice that the signer breached any duty owed to the CA or does not rightfully hold the private key used to create the signature.[254] Although the Utah Act does not provide for a presumption that the content of a digitally signed electronic record has not been altered, it does say that the other presumption only arises if a digital signature has been verified.[255] In order for a digital signature to be verified, it must be determined that the "message has not been altered since its digital signature was created."[256]

(2) The Florida and Georgia Approach: No Provision for Evidentiary Issues

Unlike the narrowly focused approach of the Utah statute, Georgia's Electronic Records and Signatures Act[257] takes a hands-off approach to issues concerning the identity of the sender of an electronic message as well as the integrity of the content of the electronic message.[258] The act does not attempt to distinguish between any

253. *See supra* text accompanying notes 208-09.
254. UTAH CODE ANN. § 46-3-406(3) (Supp. 1997).
255. *Id.*
256. *Id.* § 103(40)(b).
257. GA. CODE ANN. § 10-12-1 to -5 (Supp. 1997).
258. *Id.*

of the different forms of electronic records or electronic signatures. Furthermore, it contains no provision for any evidentiary consequences flowing from the use of any electronic signature.

Florida's Electronic Signatures Act also takes a hands-off approach to these evidentiary issues.[259] Although the Florida statute does not distinguish between various forms of electronic records or electronic signatures, the statute gives the Secretary of State the power to issue "certificates for the purpose of verifying digital signatures,"[260] but also provides that a public or private entity need not participate in the Secretary of State's certification program to verify a digital signature.[261] Thus, in both Georgia and Florida, the recipient of an electronic message faces formidable barriers to proving who was the source of the message and that the content of the message has not been altered since transmission.

(3) The Illinois Approach: An Intermediate Position

With respect to identifying the source of an electronic message, the proposed Illinois Act creates a category of signatures called a "secure electronic signature."[262] A secure electronic signature arises if it can be verified, by use of a "qualified security procedure,"[263] that "an electronic signature is the signature of a specific person."[264]

There are two forms of a qualified security procedure for identifying a party that can make an electronic signature a secure electronic signature. First, if the parties have previously agreed to use the security procedure, then a signature verified by such a procedure is a secure electronic signature.[265] Second, if a signature is verified by a security procedure approved by the Illinois Secretary of State, then it is a secure electronic signature.[266] In order for a security procedure to qualify under this method, the Secretary of State must find that the security procedure is "generally accepted in the applicable information security industry or scientific community as being capable"[267] of creating an electronic signature that

259. FLA. STAT. ANN. §§ 282.70-75 (West Supp. 1998).

260. *Id.* § 282.74.

261. *Id.*

262. Electronic Commerce Security Act, § 10-110, H.R. 3180, 90th Gen. Assembly, 1997-1998 Reg. Sess. (Ill., introduced Feb. 11, 1998), *available at* (visited Apr. 28, 1998) <http://www.mbc.com/iecsa.html>.

263. *Id.* § 10-110(a). A security procedure with respect to confirming the identity of the sender of an electronic message is "a methodology or procedure used for the purpose of . . . verifying that an electronic record is that of a specific person." *Id.* § 5-105. The qualified security procedure must be commercially reasonable under the circumstances, applied in a trustworthy manner, and relied upon reasonably and in good faith. *Id.* § 10-110(a)(1)-(3).

264. *Id.* § 10-110(a).

265. *Id.* § 10-110(b)(1).

266. *Id.* § 10-110(b)(2).

267. *Id.* § 10-135(a)(2). In making this determination, the Secretary may be guided by findings of standards organizations, such as the American National Standards Institute, the International

> is unique to the signer within the context in which it is used, can be used to objectively identify the person signing the electronic record, was reliably created by such identified person, (e.g., because some aspect of the procedure involves the use of a signature device or other means or method that is under the sole control of such person), and that cannot be readily duplicated or compromised, and is created, and linked to the electronic record to which it relates, in a manner such that if the record or the signature is intentionally or unintentionally changed after signing the electronic signature is invalidated.[268]

In addition, the Secretary may certify a qualified security procedure only if

> (1) the technology utilized by such security procedure is completely open and fully disclosed to the public, and has been so for a sufficient length of time, so as to facilitate a comprehensive review and evaluation of its suitability for the intended purpose by the applicable information security industry or scientific community; and
> (2) the technology utilized by such security procedure has been generally accepted in the applicable information security industry or scientific community as being capable of satisfying the requirements of [a secure electronic signature] in a trustworthy manner.[269]

If an electronic signature qualifies as a secure electronic signature, in a civil dispute it "shall be rebuttably presumed that the secure electronic signature is the signature of the person to whom it correlates"[270] so long as the recipient establishes that the qualified security procedure was commercially reasonable, applied in a trustworthy manner, and relied upon reasonably and in good faith.[271]

To address the issue of confirming the integrity of the content of an electronic record, the proposed Illinois Act creates a category of records called secure electronic records.[272] A secure electronic record arises when a qualified security procedure that is commercially reasonable under the circumstances, applied in a trustworthy manner, and relied upon in good faith verifies that an electronic record has not been altered since a specified point in time.[273] The proposed Illinois Act provides that a security procedure is a qualified security procedure to detect changes in the content of an electronic record if it meets either of two criteria: (1) if it is previously agreed upon by the parties;[274] or, (2) if it has been certified by the

---

Standards Organization, the International Telecommunications Union, and the National Institute of Standards and Technology. *Id.* § 10-135(b).

268. *Id.* § 10-110(b)(2)(A)-(D).
269. *Id.* § 10-135(a)(1), (2).
270. *Id.* § 10-120(b).
271. *Id.* § 10-110(a)(1)-(3).
272. *Id.* § 10-105.
273. *Id.* § 10-105(a).
274. *Id.* § 10-105(b)(1).

Secretary of State as being capable of providing reliable evidence that the content of an electronic record has not been altered.[275] The Act also provides that a digital signature certified by the Secretary of State may constitute a qualified security procedure if it meets certain other requirements.[276] If a record is a secure electronic record, then in a civil dispute it "shall be rebuttably presumed that the electronic record has not been altered since the specific point in time to which the secure status relates."[277]

d. Analysis of the Various Approaches to Verifying the Source and Content of an Electronic Message

As the foregoing discussion indicates, a number of unresolved issues among the various uniform and state law initiatives concern whether, and to what extent, to provide statutory answers to the problems of verifying the source and content of electronic messages. The next portion of this Article reviews three of these issues.

(1) Is it Appropriate to Treat Electronic Signatures and Records Verified by Security Procedures Differently from Others?

As noted, the Georgia and Florida approach does not differentiate between forms of electronic records or signatures with respect to their reliability.[278] One can make a number of arguments in favor of this hands-off approach, but they are not persuasive and are outweighed by other considerations.

One argument is that, because the Statute of Frauds does not differentiate between different types of writings based on their reliability, neither should legislation equating electronic records with signed writings. This argument is premised on the notion that electronic commerce legislation should simply equate electronic writings with paper writings. However, this argument overlooks the fact

---

275. *Id.* § 10-105(b)(2). In order to be so certified, the security procedure must be fully disclosed to the public and generally accepted in the applicable scientific or information security community. *Id.* § 10-135(a)(1), (2).

276. *Id.* § 15-101.

277. *Id.* § 10-120(a). With respect to both the presumption about secure electronic records and the presumption about secure electronic signatures, the proposed Illinois Act provides that the party against whom the presumption operates has the "burden of persuading the trier of fact that the nonexistence of the presumed fact is more probable than its existence." *Id.* § 10-120(b). Thus, the proposed Illinois Act adopts the "Morgan" or "burden-shifting" approach to presumptions. *See supra* note 244. This means that the purported sender of the message must do more than simply deny he sent the disputed message in order to avoid the mandatory effect of the presumption. Electronic Commerce Security Act, § 10-120, cmt. 3, H.R. 3180, 90th Gen. Assembly, 1997-1998 Reg. Sess. (Ill., introduced Feb. 11, 1998), *available at* (visited Apr. 28, 1998) <http://www.mbc.com/iecsa.html>.

278. Actually, the Georgia statute only relates to electronic signatures, which do have certain attributes of reliability. *See supra* text accompanying note 213. However, the Georgia statute does not provide for any evidentiary consequences of using electronic signatures, but merely provides that such a signature is a sufficient signing for state law purposes. *Id.*

that the Statute of Frauds' traditional requirement of an ink-on-paper promise provides very reliable evidence of the existence and scope of the promise sought to be enforced. By doing away with this traditional requirement, thereby allowing the Statute of Frauds to be satisfied by electronic messages with no indicia of reliability, states adopting the hands-off approach substantially undermine the evidentiary function of the Statute of Frauds.

On the other hand, statutes encouraging parties to use security procedures substantially enhance the evidentiary value of an electronic message in two ways. First, use of a security procedure assists in verifying the identity of the sender of an electronic message. In paper-based transactions, the identity of the sender of a message is indicated by the signature and its physical characteristics. Merely appending the digital equivalent of one's name at the end of an electronic message cannot serve to identify the sender because the name is merely a string of binary data that could be appended by anyone. However, security procedures of the type described in the uniform acts and the proposed Illinois Act serve as additional, reliable evidence of the identity of the sender of an electronic message.

Second, using a security procedure assists in verifying the content of an electronic message. In paper-based transactions, the integrity of the contents of the paper is usually established by the absence of visible marks of alteration or other evidence (e.g., that additions to the paper have been made by a different type of ink). Unfortunately, the digital content of an electronic message can be altered in ways that are impossible to detect. However, security procedures of the type described in the uniform acts and the proposed Illinois Act serve as very reliable evidence that the content of the message has not been altered since it was signed.

In addition, the argument that revisions to the Statute of Frauds should not differentiate between different types of electronic messages overlooks the fact that the Statute of Frauds as presently interpreted only modestly serves the earmarking and cautionary functions described by Professor Perillo.[279] The use of a security procedure, encouraged by the uniform acts and the proposed Illinois Act, would enhance these functions of the Statute of Frauds.

The use of a security procedure serves the earmarking function by assisting in the determination of when the parties have gone beyond mere negotiations and have entered into a legally enforceable promise. One would expect that parties to an electronic commerce transaction would not invoke the security procedure at a time when a potential buyer is merely browsing items at the seller's web site. Instead, the parties would invoke the security procedure only at the time the party were prepared to consummate the transaction. Hence, if the parties have used a security procedure to verify an electronic message, that should constitute persuasive evidence that the parties thought the message sufficiently important to go beyond mere negotiation.[280]

---

279. Perillo, *supra* note 146, at 48-56.

280. Of course, because of other requirements for contract enforceability, such as consideration, the use of a security procedure to authenticate an electronic message would not fully serve the earmarking function. *See id.* at 50.

Likewise, the use of a security procedure serves the cautionary function of warning the parties that they are entering into a legally enforceable transaction just as the act of signing one's name to a piece of paper serves the same purpose. The act of invoking a security procedure emphasizes the fact that one is entering into a transaction with potential legal consequences. Hence, treating electronic messages verified by a security procedure differently than unverified messages encourages the use of a security procedure and serves some functions not currently served by the Statute of Frauds.

Another argument in favor of the hands off approach of the Florida and Georgia statutes is that the market for security procedures in electronic commerce is in its infancy and any attempt to regulate the type of security procedures that receive special treatment in electronic commerce is premature. According to this argument, the free market will inevitably find the most efficient way to internalize the costs associated with the risk of electronic commerce and any interference with that market skews the result. This argument has substantial effect when directed at statutes like the one enacted in Utah, which singles out only digital signatures for special treatment. However, the argument loses much of its force when applied to statutes that allow the parties to agree to the use of security procedures and to treat such agreed-upon procedures differently because the agreement reflects the action of market forces.

Finally, encouraging the use of security procedures minimizes the number of electronic commerce disputes that result in litigation. If a message has been sent by an impostor or been tampered with in transit, or if a message has simply been corrupted in the course of transmission, reliable security procedures should indicate to the recipient that something is amiss. If the message cannot be verified by the security procedure, then the recipient will probably attempt to contact the purported sender and inquire about the message before relying on it. This should limit the number of controversies arising from electronic commerce transactions.

(2) What Security Procedures Are Sufficiently Reliable to Merit Special Treatment?

Assuming that it is proper for a state to encourage the use of security procedures in electronic commerce, what forms of security procedures should qualify for special legislative treatment? Once again, there has been disagreement among the uniform and state laws addressing this issue. The Utah statute is limited to digital signatures, the uniform law focuses on security procedures agreed to by the parties, and the Illinois approach includes security procedures previously agreed on by the parties and other administratively certified security procedures.

(a) Digital Signatures Alone

Undoubtedly, digital signatures provide the most reliable method of identifying the source and verifying the content of an electronic message. Digital signature

technology has been subjected to intense scrutiny in the information security industry for more than a decade and found to be essentially fool-proof, so long as it is based on appropriate algorithms, the subscriber safeguards his private key, and the certification authority acts to reliably identify the subscriber. The Utah legislature was certainly justified in concluding that most messages verified by a digital signature are sufficiently reliable to be entitled to enhanced evidentiary status. However, by according this status only to digital signatures, the Utah approach suffers from some serious problems.

First, the Utah statute discourages the development and adoption of other forms of security procedures.[281] The Utah statute leaves other forms of electronic messages in a legal limbo, because it is unclear whether any such electronic message could even satisfy the requirements of the Statute of Frauds.[282] Even if some other form of electronic message might satisfy the Statute of Frauds, by specifying digital signatures as the sole form of security procedure giving rise to evidentiary presumptions as to the source and content of the electronic message, the Utah statute gives digital signatures a substantial competitive advantage over other security procedures. Potential purchasers of security systems may conclude that other security procedures are necessarily unreliable merely because they are omitted from the statute. Furthermore, even if a new security procedure develops that provides identical, or even superior, reliability, such technology will face substantial barriers to market entry. These barriers can only be overcome by the enactment of legislation giving the new technology a status similar to digital signatures.

Second, the Utah statute is premised on the assumption that the digital signature is the *only* presently available and commercially reasonable form of electronic communication. It may be true that the digital signature is the only presently available method of reliably verifying the source and content of an electronic message in cases involving stranger-to-stranger transactions. However, a substantial amount of electronic commerce is carried on by parties who have repeated dealings with each other. In such cases, the parties should be free to adopt their own form of security procedure. If the procedure is commercially reasonable, then their agreement should be encouraged by giving enhanced evidentiary effect to the message verified by the parties' chosen security procedure.

Third, the Utah statute treats all digital signatures alike, regardless of the level of security afforded by the algorithms underlying them. Presently, there are two widely accepted public algorithms used in digital signatures, the RSA (Rivest-Shamir-Adelman) algorithm and the DSA (Digital Signature Algorithm) algorithm.[283] However, earlier, shorter forms of the RSA algorithm have been successfully factored by a concerted effort of scientists and students utilizing idle processor time on a great number of computer workstations.[284] Likewise, a new form of

281. *See* Winn, *supra* note 18.

282. *See supra* text accompanying notes 208-09.

283. FORD & BAUM, *supra* note 1, at 109-15.

284. *Id.* at 110. The algorithm that was successfully factored was a 129-digit (429-bit) modulus

cryptosystem, called an elliptical curve cryptosystem, is a variant of other cryptosystems that depend upon a discrete logarithm problem.[285] The elliptical curve has been studied for several years and appears promising as a basis for digital signatures, but it does not yet have the same level of acceptance in the information security community as the RSA and DSA algorithms. The Utah statute treats all digital signatures alike, regardless of the strength or level of acceptance of the underlying algorithms.[286]

Finally, the Utah statute implements extensive regulation of certification authorities (CAs). The Utah Division of Corporations and Commercial Code (Division) of the Utah Department of Commerce is given the power both to act as a CA itself and to license other CAs.[287] CAs must meet detailed licensure requirements designed to provide evidence of reliability, trustworthiness, and financial stability and are subject to annual performance audits.[288] Finally, the CA must provide a "suitable guaranty" in the form of a surety bond or a letter of credit in a form and amount specified by the Division.[289] Although CAs play a critical role for digital signatures, this extensive regulation increases the cost of digital signature technology and discourages its use, thus retarding the development of a robust electronic commerce market based on reliable forms of electronic communication.

(b) Security Procedure Agreed to by the Parties

The uniform acts' focus on security (or attribution) procedures agreed to by the parties serves to further the notion of freedom of contract and avoids the problem of the Utah statute's attempt to specify a particular technology as the sole, secure form of engaging in electronic commerce. If the parties are free to adopt an attribution procedure, they will adopt one that is appropriate to the risk posed by their

---

that had been posted as a public challenge by the inventors of the RSA algorithm in 1977. The RSA algorithm is considered safe, nonetheless, because a relatively small increase in the size of the RSA modulus results in a large increase in the effort required to factor it. *Id.*

285. *Id.* at 116-17.

286. The Utah statute indirectly places limits on the types of digital signatures that fall within its scope. The term "digital signature" is defined as

> a transformation of a message using an asymmetric cryptosystem such that a person having the initial message and the signer's public key can accurately determine whether: (a) the transformation was created using the private key that corresponds to the signer's public key; and (b) the message has been altered since the transformation was made.

UTAH CODE ANN. § 46-3-103(10) (Supp. 1997). The statute defines "asymmetric cryptosystem" as "an algorithm or series of algorithms which provide a secure key pair." *Id.* § 103(2). Although the term "secure" is not defined, a digital signature based on an algorithm known to be insecure may not qualify as a "digital signature" because it cannot generate a secure key pair. It is unclear whether the drafters of the Utah statute intended the proponent of a digitally-signed document to have the burden of proving that the digital signature was created using an asymmetric cryptosystem as defined in the statute.

287. *Id.* § 104(1).

288. *Id.* §§ 201, 202.

289. *Id.* § 201(1)(d).

contemplated transactions. Hence, it may be something as complex as a digital signature or something as simple as a PIN number.

Two difficulties arise with an approach based on the use of attribution procedures agreed to by the parties. The first is the difficulty posed by an economically-dominant party insisting on the use of an inappropriate security procedure. This difficulty is dissipated by the uniform acts' requirements that the security procedure be commercially reasonable and that the recipient of an electronic message exercise good faith and reasonably rely on the security procedure.[290] These limitations should prevent most forms of overreaching.

The second difficulty, however, is one for which there appears to be no remedy. In order for the uniform acts' provisions to apply, the security procedure must be agreed to (or adopted) by the parties. It is unclear how one proves the initial agreement to use the attribution procedure. If there were a requirement that the attribution procedure be previously agreed upon by the parties, then independent evidence of the identity of the party arising from the agreement to use the attribution procedure would exist. This would justify presuming that subsequent messages verified by the attribution procedure did, in fact, come from that party. However, the commentary to section 2B-114 indicates that an attribution procedure need not be previously agreed upon by the parties. This commentary provides:

> On the other hand, agreement or adoption need not precede the transaction involved. Parties dealing for the first time may adopt a procedure for authentication of messages. That adopted procedure would have the full force of an attribution procedure it if is commercially reasonable.[291]

This commentary is puzzling. On the one hand, it suggests that no prior agreement to use the security procedure is necessary. However, if the parties send a series of electronic messages as part of a single transaction, it would be extremely difficult for the recipient of the message to prove the identity of the person who, in one of the earlier messages, agreed to use an attribution procedure. Certainly, the drafters could not have intended to allow the recipient of the message to use an attribution procedure to prove the identity of the other party for the purpose of showing who initially agreed to the use of the attribution procedure. Such a result would be perfectly circular.

Alternatively, this commentary might imply that the recipient of a series of messages might take other measures to identify the source of an electronic message after an exchange of messages and that such other measures might be sufficient to establish the identity of the person agreeing to the attribution procedure. For example, the recipient might ask for a street address, telephone number, or other identifying information that could subsequently be confirmed by reference to an

290. U.C.C. § 2B-116(a)(2) (Proposed Draft Apr. 15, 1998); UETA, *supra* note 184, § 202(a)(2).

291. U.C.C. § 2B-114 reporter's note 2 (Discussion Draft Apr. 15, 1998).

independent third party. However, in such a case the recipient would have independent evidence of the identity of the person and this would undercut the need for the presumption flowing from the use of the attribution procedure in the first place.

In short, the effect of the attribution procedure in light of this commentary is unclear. The thrust of Article 2B and the UETA is that the parties should be free to agree on an attribution procedure and, so long as it is commercially reasonable, the use of that procedure to indicate the identity of the sender should have the effect of giving rise to a presumption as to the identity of the sender. This result and the reasoning behind it make perfect sense in cases where the parties agree to use an attribution procedure in contemplation of a series of future transactions. However, in stranger-to-stranger transactions, it is difficult to see how one could prove the existence of an attribution procedure by agreement.[292] If that is the case, then the presumption flowing from use of an attribution procedure may be limited to cases where parties to an electronic message have a prior course of dealing and will have little or no utility in stranger-to-stranger transactions.[293]

(c) Security Procedures Previously Agreed to by the Parties and Other Reliable Security Procedures

The proposed Illinois Act recognizes two ways in which a security procedure can be a qualified security procedure for purposes of identifying the source of an electronic message. First, it includes a security procedure "previously agreed to by the parties."[294] This provision is similar to the approach of the uniform acts, but it limits the security procedures to those that are previously agreed to. The basis for this limitation is the inherent difficulty of proving an agreement of the parties to use a security procedure when that agreement is part of a single series of electronic messages.[295] By requiring a previous agreement, the proposed Illinois Act requires that there be some way of proving the identity of the person originally agreeing to the use of a security procedure before subsequent messages verified by the security procedure would be attributable to that person. Once the original agreement is established, subsequent communications between the parties using this security procedure allow the recipient to verify the sender's identity by use of the security procedure. The recipient is entitled to a presumption that the sender did send the

---

292. It would, of course, be possible to show that the parties had used an attribution procedure otherwise established by law, but that is not what the commentary to section 2B-114 states. *Id.*

293. Of course, the drafters of Article 2B may have believed that stranger-to-stranger transactions would rarely involve an amount of money ($20,000) that would trigger Proposed Article 2B's Statute of Frauds provision. *Id.* § 2B-201(a)(2)(B).

294. Electronic Commerce Security Act §§ 10-105(b)(1), 10-110(b)(1), H.R. 3180, 90th Gen. Assembly, 1997-1998 Reg. Sess. (Ill., introduced Feb. 11, 1998), *available at* (visited Apr. 28, 1998) <http://www.mbc.com/iecsa.html>.

295. This difficulty was previously discussed in connection with the provisions of proposed Article 2B. *See supra* text accompanying notes 292-93.

message, so long as the security procedure was commercially reasonable, used in a trustworthy manner, and was relied upon reasonably and in good faith.[296] By so limiting this class of qualified security procedures, the Illinois Act sends a clear message that this form of qualified security procedure will not arise in cases of stranger-to-stranger transactions.

In order to encourage the development and implementation of security procedures that could be utilized in stranger-to-stranger transactions, the proposed Illinois Act creates a second class of "qualified security procedure"—any security procedure certified by the Illinois Secretary of State according to standards set forth in the Act.[297] Initially, the proposed Illinois Act also included digital signatures as a third class of "qualified security procedure."[293] However, the drafters deleted digital signatures due to the difficulty of differentiating which forms of digital signature are based on sufficiently reliable algorithms and which are not. In other words, the drafters realized that not all digital signatures are alike and that the job of sorting out the reliable from the unreliable ones requires a level of expertise best left to administrative evaluation. Furthermore, the drafters were persuaded that specifying a particular form of digital signature in the statute—for example, only those based on a 1024-bit RSA algorithm—might deter the development of other security procedures, grant an undue competitive advantage to particular implementations of digital signatures, and be rendered inaccurate by subsequent developments. Nevertheless, the statute contemplates that at least some forms of digital signatures are likely candidates for certification by the Secretary.[299]

Instead of attempting to determine precisely what types of security procedures might qualify, the proposed Illinois Act establishes neutral standards for determining what forms of security procedures should be certified as a qualified security procedures. By establishing standards, the proposed Illinois Act is technologically neutral, yet gives sufficient guidance to interested parties regarding the characteristics that will be required of a security procedure before it can be certified. Furthermore, this procedure allows for an on-going review of new security procedures which may be developed and does not require amendment of the statute to recognize these technologies. This approach presents two principal issues: what standards should guide the decision about security procedures?; and, which decision-making body should have the power to approve these security procedures?

The proposed Illinois Act contains a number of requirements for the first of these

---

296. Electronic Commerce Security Act § 10-110(a)(1)-(3), H.R. 3180, 90th Gen. Assembly, 1997-1998 Reg. Sess. (Ill., introduced Feb. 11, 1998), *available at* (visited Apr. 28, 1998) <http://www.mbc.com/iecsa.html>.

297. *Id.* §§ 10-105(b)(2), 10-110(b)(2).

298. Illinois Electronic Commerce Security Act § 302(b)(1) (Discussion Draft Nov. 15, 1997).

299. Electronic Commerce Security Act, § 15-105, H.R. 3180, 90th Gen. Assembly, 1997-1998 Reg. Sess. (Ill., introduced Feb. 11, 1998), *available at* (visited Apr. 28, 1998) <http://www.mbc.com/iecsa.html>. This section provides that, if the Secretary certifies a digital signature as a qualified security procedure, additional facts should be established before the digitally signed message is entitled to the statutory presumptions of genuineness.

issues. The goal of these standards is to describe the attributes of a security procedure that would provide a reliable method of identifying the source of an electronic message in a stranger-to-stranger transaction. Hence, the proposed Illinois Act requires that, before the Secretary certifies a new security procedure,

> the technology utilized by such security procedure is completely open and fully disclosed to the public and has been so for a sufficient length of time so as to facilitate a comprehensive review and evaluation of its suitability for the intended purpose by the applicable information security industry or scientific community.[300]

This requirement not only enhances the evaluation of the security procedure, but also serves to more widely disseminate information about security procedures. Furthermore, the Act requires that the technology be "generally accepted in the applicable information security industry or scientific community" as meeting the standards of the act.[301] This requirement has the salutary effect of requiring the Secretary to consider whether the experts in the area have arrived at a consensus and also prevents the hasty certification of a security procedure that might be touted as reliable by its proponents, but not yet accepted by disinterested third-party experts.

With respect to secure electronic records, the security procedure must be "capable of providing reliable evidence that an electronic record has not been altered."[302] Regarding secure electronic signatures, a security procedure must be capable of creating an electronic signature that is unique to the signer, can be used to objectively identify the sender, was reliably created by the sender, and is reliably linked to the electronic record.[303] These are rigorous standards indeed, but they are necessary because a certified security procedure will have the enhanced evidentiary effect of presumptions of genuineness even if there is no prior agreement by the parties for its use. As such, the security procedure must be one that can be reliably used by parties in a stranger-to-stranger transaction.

The second issue of who should determine whether a security procedure qualifies under the relevant standards is also a difficult one. Ideally, a national or international accrediting body comprised of scientists or information security experts might come into existence and develop standards for security procedures in electronic commerce. However, that development is years, if not decades, in the future. Hence, if provision is to be made for security procedures in stranger-to-stranger transactions, each state should attempt to resolve the issue.

One alternative would be to leave the issue to the judiciary. A legislature could promulgate standards, and leave to the courts the determination, on a case-by-case basis of whether a security procedure meets those standards. However, this approach

---

300. *Id.* § 10-135(a)(1).
301. *Id.* § 10-135(a)(2).
302. *Id.* § 10-105(b)(2).
303. *Id.* § 10-110(b)(2)(A)-(D).

has significant shortcomings. First, it would likely deter the development of alternative security procedures. In order to receive the sanction of a judicial decision, someone would have to utilize the new security procedure in a transaction with enough money at stake to justify litigation through the appellate level. It is unlikely that a private party would have the incentive to do this.[304] Second, the judiciary has very limited fact-finding capability and would be limited to the evidence presented by the parties. In this situation, it is more desirable that the decision-making body have independent fact-gathering means, in order to take advantage of the expertise available in the information security industry.

A second alternative is to require the proponents of each new technology to persuade the legislature to amend the statute to include the new technology as a secure electronic record or signature. This would require the proponents of the security procedure to gain the ear of the legislature in each state, a matter that has been difficult enough with respect to other, more basic electronic commerce issues.

The final alternative is some form of administrative action. This would allow the administrative agency to employ experts necessary to evaluate the procedure, take advantage of the knowledge in the information security industry,[305] and for competing views to be aired in the normal rule-making process. Furthermore, the rate of change in the area of information security is fast paced. As older, once-reliable security procedures are proven to have flaws, new or improved security procedures will emerge to take their place. Allowing administrative determination of what security procedures should be qualified provides an ongoing review of new technologies without the need for statutory amendment. Additionally, provision should be made for decertifying a security procedure if subsequent developments show that it is no longer capable of performing the functions listed in the statute.[306] All of these considerations suggest that an administrative body is likely the best entity to determine the difficult questions of what security procedures should to qualify for special treatment.

(3) Is an Evidentiary Presumption a Proper Way to Encourage the Use of Security Procedures?

Assuming that it is proper for a legislature to encourage the use of more secure forms of electronic communication, is it appropriate to encourage that use by affording to records and signatures, verified by a security procedure a rebuttable

304. Of course, the developer of the security procedure would have a powerful incentive to instigate a collusive lawsuit between two of its cronies, who might create a dispute solely for the purpose of putting forward evidence favorable to the security procedure.

305. The proposed Illinois Act specifically provides that the Secretary may be guided by finding of a number of recognized national and international standards-setting bodies. Electronic Commerce Security Act § 10-135(b), H.R. 3180, 90th Gen. Assembly, 1997-1998 Reg. Sess. (Ill., introduced Feb. 11, 1998), *available at* (visited Apr. 28, 1998) <http://www.mbc.com/iecsa.html>.

306. *Id.* § 10-135(d).

presumption that the record has not been altered and that the signature is that of the person indicated by the security procedure? Virtually all of the traditional justifications underlying evidentiary presumptions are present with respect to using a security procedure to verify the source and content of an electronic record.

First, because of the requirements that the security procedure be commercially reasonable and reasonably relied upon in good faith, proof of the predicate fact (use of a security procedure to verify the source and content of an electronic message) is a highly reliable indicator of the existence of the presumed facts (the person indicated by the security procedure did send the message and that it has not been altered). The most important consideration in the creation of a presumption is its probability.[307]

Second, absent the presumption, it will be very difficult for the recipient of an electronic message to prove the source and content of the electronic message. Unless the parties have a history of prior transactions, the recipient will not likely have any evidence of the source and content of the message other than the results of the security procedure and the reliability of that procedure. Presumptions are frequently justified by the difficulties inherent in proving that the more probable event occurred.[308]

Third, the evidence which would indicate that someone other than the purported sender sent the message is almost exclusively in possession of the purported sender. For example, the usual reason why a security procedure would misidentify the actual sender of an electronic message is that someone has stolen or compromised the defendant's access code, private key, or other method of identifying himself to the recipient. Because the evidence about these matters is much more accessible to the purported sender of the electronic message rather than the recipient, the presumption is justified to correct the imbalance resulting from the purported sender's superior access to proof of the issues.[309]

Finally, because the recipient's use of the security procedure to verify the source and content of the electronic message occurs before the recipient acts in reliance on the message, the recipient's caution should be rewarded. This will prevent many disputed electronic commerce transactions from reaching the courtroom. When the recipient cannot verify the source or content of an electronic message by using the security procedure, he will likely seek some form of clarification about this before the recipient acts on the message (by shipping the product, extending credit, etc.). Hence, the presumption is justified as rewarding this type of prereliance verification by easing the recipient's burden of proof in the event of a dispute regarding the identity of the sender. Presumptions are frequently created to encourage certain

---

307. *See, e.g.*, MCCORMICK ON EVIDENCE, *supra* note 244, § 343, at 580. (stating that "[m]ost presumptions have come into existence primarily because the judges have believed that proof of fact B renders the inference of the existence of fact A so probable that it is sensible and timesaving to assume the truth of fact A until the adversary disproves it").

308. *Id.*

309. *Id.*

social or economic policies.[310] The policy of adopting appropriate security procedures to verify the source and content of an electronic message before acting on it would certainly seem to be a policy worthy of encouragement.

VI. CONCLUSION

Electronic commerce on the Internet has such enormous potential that it will continue to develop, regardless of how legislatures treat the issues raised by the Statute of Frauds. However, electronic commerce on the Internet can best be fostered by carefully drafted statutes which remove barriers to electronic commerce and also encourage the use of security procedures that provide protection from the possibilities of fraud inherent in electronic commerce and the open, free networks over which such commerce takes place. These improvements can be achieved without stifling future technological development and without inhibiting the parties' freedom of contract. A middle-ground statute, like the proposed Illinois Act, will go far to enhance the development of electronic commerce on the Internet as an efficient, yet safe, method of doing business.

310. *Id.*